SANGFOR VDC 4.1 用户手册

2015 年 3 月

目录

声明

前言

手册内容

第 1 部分 SANGFOR VDC 产品概述。该部分主要介绍 VDC 设备的外观特点和使用环境，以及连接前的准备和注意事项。

第 2 部分 SANGFOR VDC 设备的安装部署。

第 3 部分 SANGFOR VDC 设备的使用。

本手册以深信服 VDC 2500 为例进行配置。各型号产品硬件规格存在一定差异，但是配置以及使用方法是一样的，所有涉及产品规格的问题需要和深信服公司联系确认。

本书约定

图形界面格式约定

文字描述	代替符号	举例
按钮	边框+阴影+底纹	“确定”按钮可简化为确定
菜单项	『 』	菜单项“系统设置”可简化为『系统设置』
连续选择菜单项及子菜单项	→	选择『系统设置』→『接口配置』
下拉框、单选框、复选框选项	[ ]	复选框选项“启用用户”可简化为[启用用户]
窗口名	【】	如点击弹出[新增用户]窗口
提示信息	“”	提示框中显示“保存配置成功，配置已修改,需要重启 DLAN 服务才能生效，是否立即重启该服务?”

各类标志

本书还采用各种醒目标志来表示在操作过程中应该特别注意的地方，这些标志的意义

如下：

 **小心、注意：**提醒操作中应注意的事项，不当的操作可能会导致设置无法生效、数据丢失或者设备损坏。

 **警告：**该标志后的注释需给予格外的关注，不当的操作可能会给人身造成伤害。

 **说明、提示、窍门：**对操作内容的描述进行必要的补充和说明。

技术支持

用户支持邮箱：	support@sangfor.com.cn
技术支持热线电话：	400-630-6430（手机、固话均可拨打）
技术支持论坛：	http://sangfor.360help.com.cn/
公司网址：	http://www.sangfor.com.cn

致谢

感谢您使用我们的产品及用户手册，如果您对我们的产品或用户手册有什么意见和建议，您可以通过电话、论坛或电子邮件反馈给我们，我们将不胜感谢。

第1章 VDC 设备的安装

本部分主要介绍了 SANGFOR VDC 系列产品的硬件安装。硬件安装正确之后，您才可以进行配置和调试。

1.1. 环境要求

VDC 设备可在如下的环境下使用。

输入电压： 110V～230V

温度： 0～45℃

湿度： 5～90％

为保证系统能长期稳定地运行，应保证电源有良好的接地措施、防尘措施，保持使用环境的空气通畅和室温稳定。本产品符合关于环境保护方面的设计要求，产品的安放、使用和报废应遵照国家相关法律、法规要求进行。

1.2. 电源

SANGFOR VDC 系列产品使用交流 110V 到 230V 电源。在您接通电源之前，请保证您的电源有良好的接地措施。

1.3. 产品外观

图 1 SANGFOR VDC 网关面板（以 VDC 2500 为例）

从左到右的指示灯分别是：

ETH0 LINK: 用于显示 LAN 口线路连接情况

ETH0 ACT: 对应显示 LAN 口数据流量情况

ETH2 LINK: 用于显示 WAN1 口线路连接情况

ETH2 ACT: 对应显示 WAN1 口数据流量情况

ETH1 LINK: 用于显示 DMZ 口线路连接情况

ETH1 ACT: 对应显示 DMZ 口数据流量情况

ETH3 LINK: 用于显示 WAN2 口线路连接情况(多线路产品才能使用此接口)

ETH3 ACT: 对应显示 WAN2 口数据流量情况

POWER: VDC 2500 设备电源指示灯

ALARM: VDC 2500 设备报警指示灯(设备启动时一分钟内长亮)

图片仅供参考，不同型号的产品外观请以实物为准。

1.4. 配置与管理

在配置网关之前，您需要配备一台电脑，配置之前请确定该电脑的网页浏览器能正常使用，然后把电脑与 SANGFOR VDC 连接在同一个局域网内，通过网络对设备进行配置。

1.5. 设备接线方式

在背板上连接电源线，打开电源开关，此时前面板的 Power 灯（绿色，电源指示灯）和 Alarm 灯（红色，告警灯）会点亮。大约 1-2 分钟后 Alarm 灯熄灭，说明网关正常工作。

请用标准的 RJ-45 以太网线将 ETH0 口与内部局域网连接，对 VDC 设备进行配置。

请用标准的 RJ-45 以太网线将 ETH2 口与 Internet 接入设备相连接，如路由器、光纤收发器或 ADSL Modem 等。

注意：多线路的 VDC 设备可以支持多条 Internet 线路，此时可将 ETH3 口与第二条 Internet 接入设备相连，ETH4（WAN3）口与第三条 Internet 线路相连，依此类推。

使用标准 RJ-45 以太网线将 ETH1 口与 DMZ 区的网络连接，一般而言，DMZ 区放置

对外提供服务的服务器。VDC 设备可以为这些服务器提供安全保护。

VDC 设备正常工作时 POWER 灯常亮，ETH0 口和 ETH2 口 LINK 灯长亮，ACT 灯在有数据流量时会不停闪烁。ALARM 红色指示灯只在设备启动时因系统加载会长亮（约一分钟），正常工作时熄灭。如果在安装时此红灯长亮，请将设备断电重启，重启之后若红灯一直长亮不能熄灭，请与深信服联系。

ETH2（WAN）口直接连接 MODEM 应使用直连线、连接路由器应使用交叉线；ETH0（LAN）口连接交换机应使用直通线、直接连接电脑网口应使用交叉线。当指示灯显示正常，但不能正常连接的时候，请检查连接线是否使用错误。直连网线与交叉网线的区别在于网线两端的线序不同，如下图：

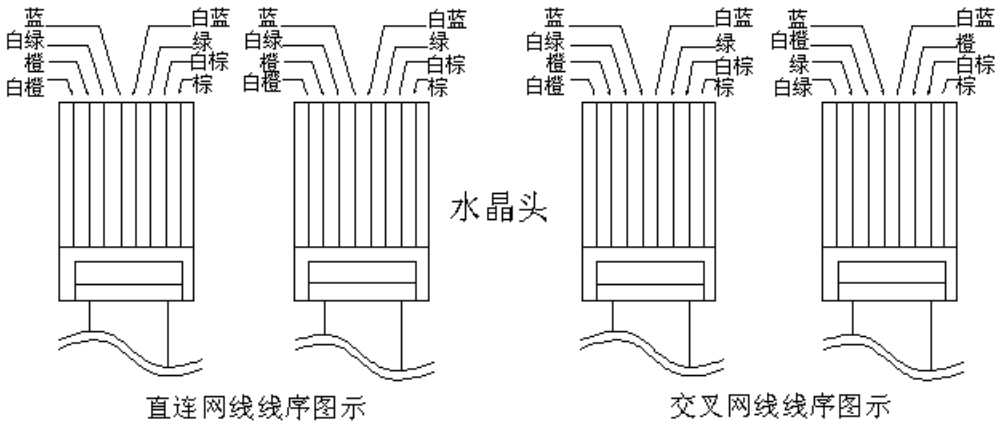


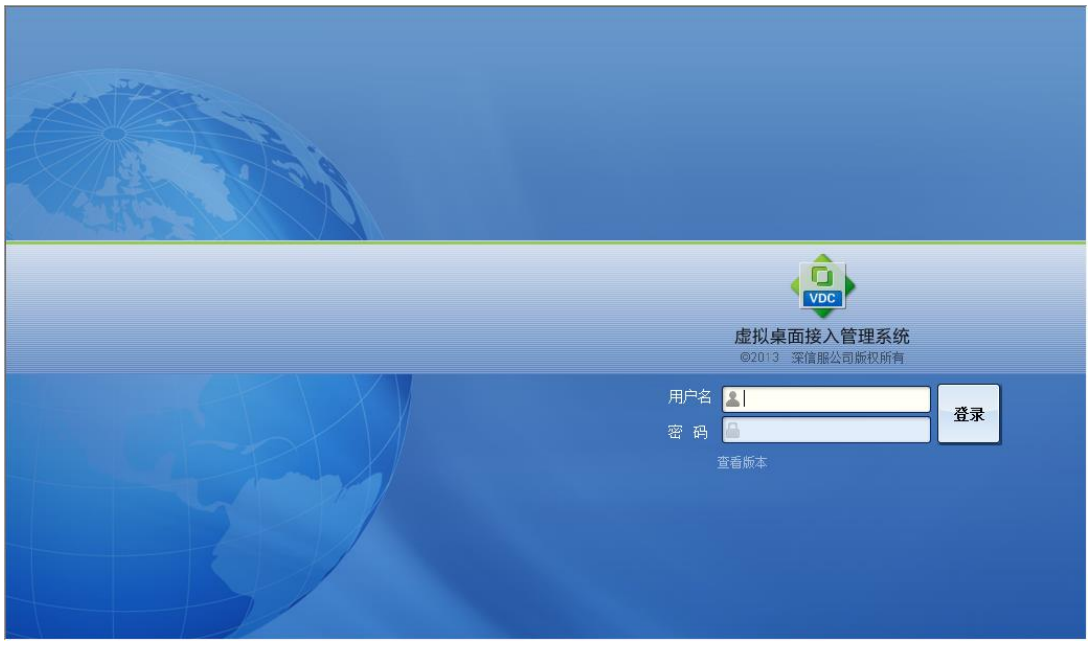
图 2 直连线、交叉线 线序

第2章 控制台的使用

2.1. 登录 WebUI 配置界面

按照前面所示方法接好线后，通过 Web 界面来配置 VDC 设备。方法如下：

首先为本机器配置一个 10.254.254.X 网段的 IP（如配置 10.254.254.100），掩码配置为 255.255.255.0，然后在 IE 浏览器中输入网关的默认登录 IP 及端口，输入 https://10.254.254.254:4430，页面如下：



在登录框输入『用户名』和『密码』，点击登录按钮即可登录 VDC 控制台进行配置，默认情况下的用户名和密码均为：admin，注意区分大小写。

如果需要查看当前网关的版本号，可点击查看版本，即显示当前硬件的版本信息。

登录 WebUI 控制台后，可以看到有以下配置内容：

如下图所示：

『运行状态』：此处可以查看当前设备的运行状态。

『系统设置』：此处可设置设备的序列号、网络配置及各种常见全局性配置。

『VDI 设置』：设置虚拟桌面相关信息。

『防火墙设置』：设置设备内置的防火墙规则及策略。

『系统维护』：用来查看日志、备份/恢复设备的配置信息，重启设备/服务或关闭设备。

注意：所有配置界面中如果有[确定]、[保存]、[配置生效]按钮，则配置完毕后，必须要点击该按钮才能使设置保存并生效，后面的文档不再赘述。

2.2. 运行状态

『VDI 运行状态』里面可以查看『系统状态』，『在线用户』，『告警日志』，『终端服务』。界面如下图所示：

2.2.1. 系统状态

在『系统状态』里面可以选择查看相应的模块，包括：『系统信息』，『链路状态』，『网络吞吐量』，『并发用户趋势』，『并发会话数』。

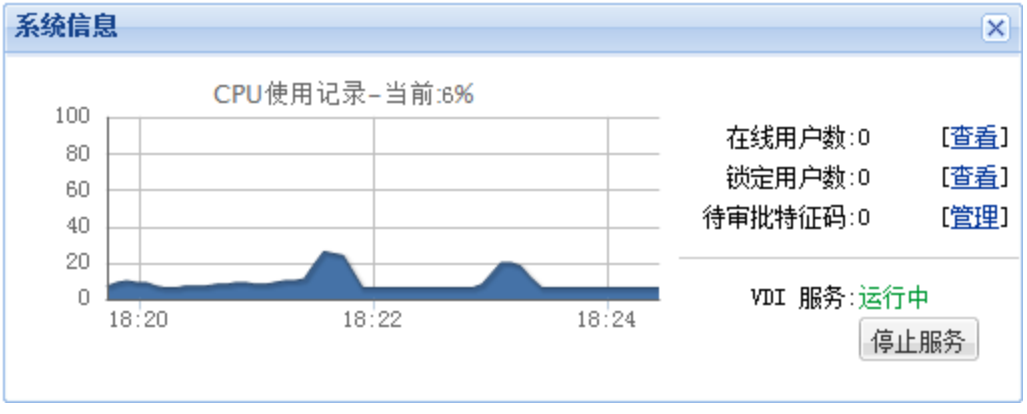
WEBUI 路径：『运行状态』→『VDI 运行状态』→『系统状态』。

界面如下图所示：

点击[选择模块]右边的，在相应的模块前打钩，勾选的模块就会在页面空白处显示。

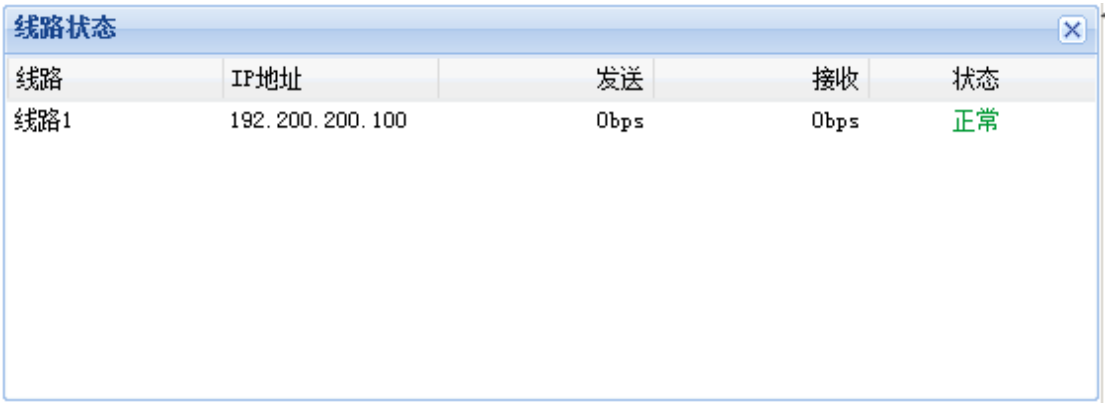
『刷新间隔』，设置页面信息的刷新时间。点击立即更新，则立即更新页面上显示的信息。

『系统信息』，可以查看相应的 CPU 使用记录、在线用户数、锁定用户数、待审批特征码、VDI 服务状态，点击后面的查看，可以分别链接到在线用户列表页面、锁定用户列表页面和特征码管理页面。显示如下：

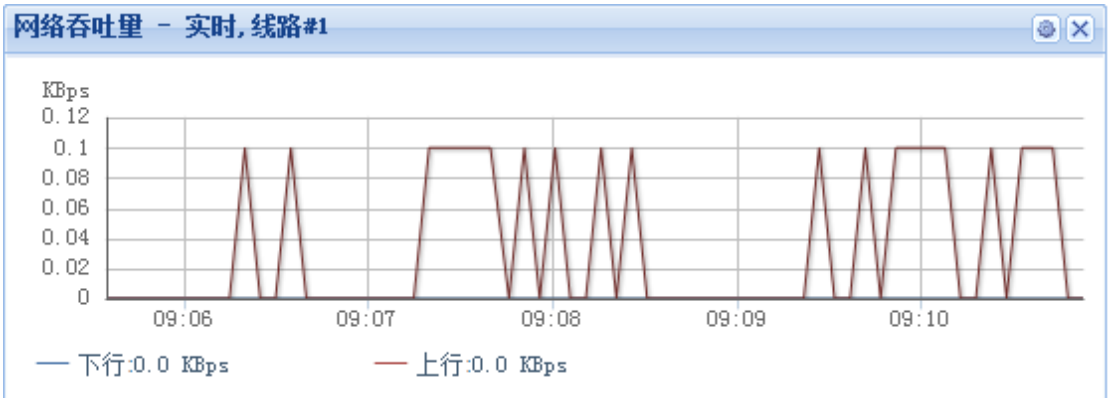


点击停止服务，停止 VDI 服务。

『线路状态』，可以查看所有外网线路的状态信息，并且可以看到相应线路的流速大小。显示如下：



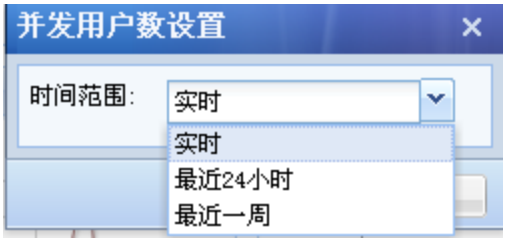
『网络吞吐量』，可以查看线路的流速大小，显示如下：



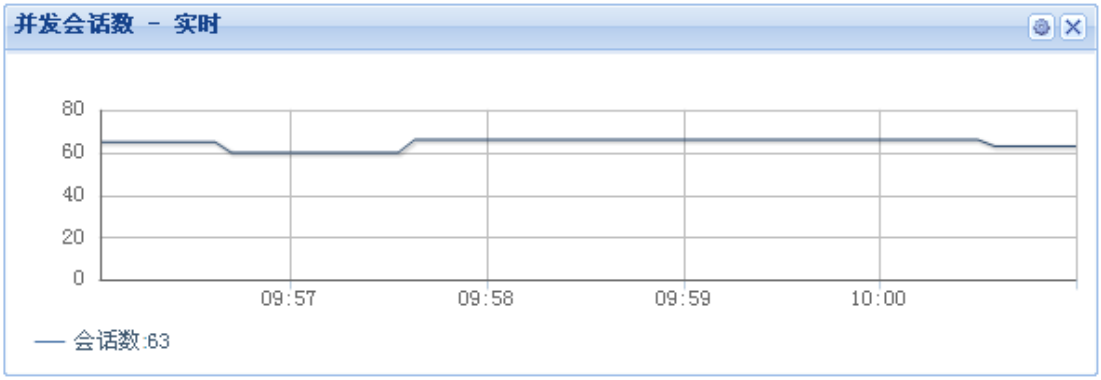
点击右上角图标  ，选择查看的时间范围（实时；最近 24 小时；最近一周），线路，显示流速的单位。如下图：

『并发用户趋势』可以查看某个时间段内登录 VDI 的用户数。显示如下：

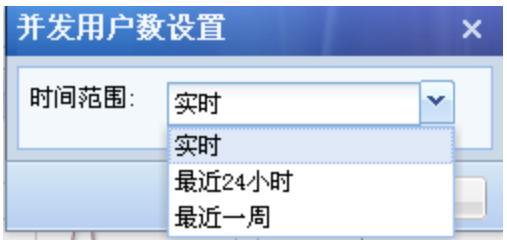
点击左上角的编辑图标，能够选择实时，最近 24 小时，最近一周时间段来显示，显示如下：



『并发会话数』可以查看当前或选择时间段设备发起的并发会话数。显示如下：



点击左上角的编辑图标，也可以选择实时，最近 24 小时，最近一周时间段来显示会话数，显示如下：



2.2.2. 在线用户

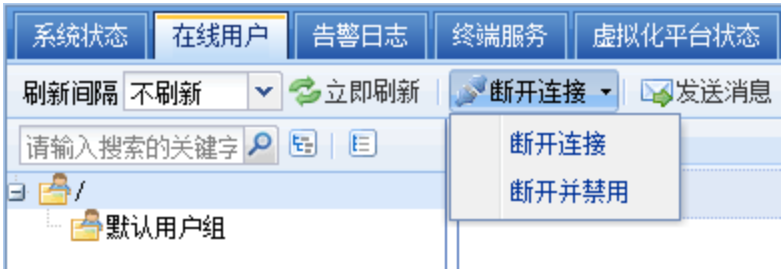
在『在线用户』里面可以查看当前登录的 VDI 在线用户，可以查看到相应用户的接收发送流速/流量和接入 VDI 的时间，可以手动将接入的 VDI 用户断开或禁用。

WEBUI 路径：『运行状态』→『VDI 运行状态』→『在线用户』。

界面如下图所示：

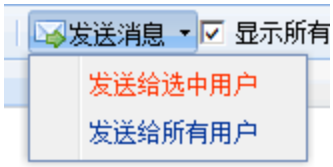
『刷新间隔』可以设置页面自动刷新时间，点击立即刷新则立即刷新页面信息。

点击断开连接可选择[断开连接]或者[断开并禁用]。页面显示如下：

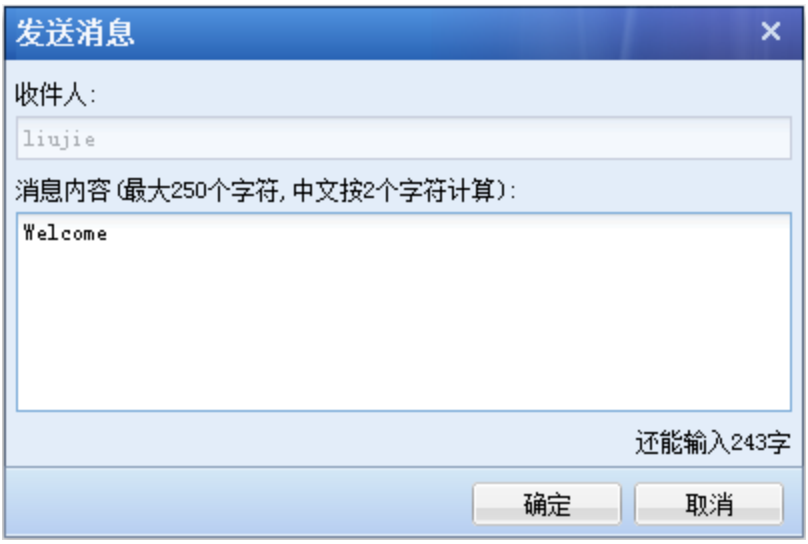


勾选相应的用户，然后点击『断开连接』，该用户则断开 VDI 的连接。如果选择『断开并禁用』，并点击立即生效，则该用户被断开后将被禁止登录。

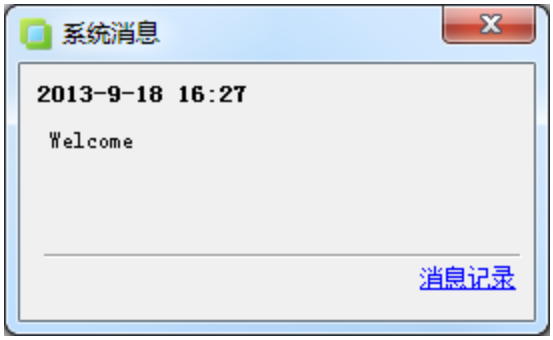
点击发送消息，给 VDI 用户发送相应的信息，可以选择[发送给选中用户]或者[发送给所有用户]，如下图：



选择用户对象后，可设置消息内容，显示如下：



点击确定后，VDI 客户端登陆后，在屏幕右下角，会弹出相应消息，显示如下：

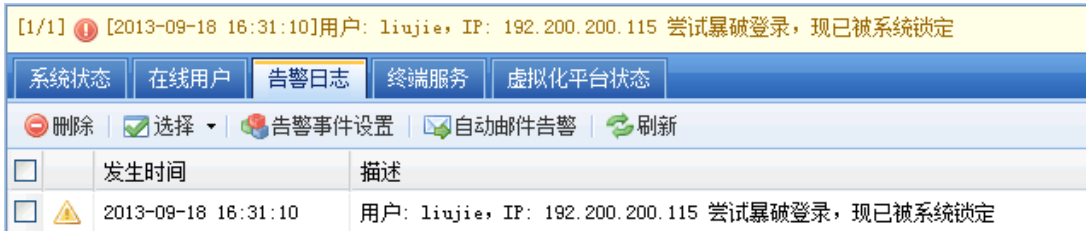


2.2.3. 告警日志

『告警日志』里面可以查看 VDC 设备的相应告警信息。

WEBUI 路径：『运行状态』→『VDI 运行状态』→『告警日志』。

显示如下：



点击删除，则可以将选择的告警日志从下面的列表中删除掉。

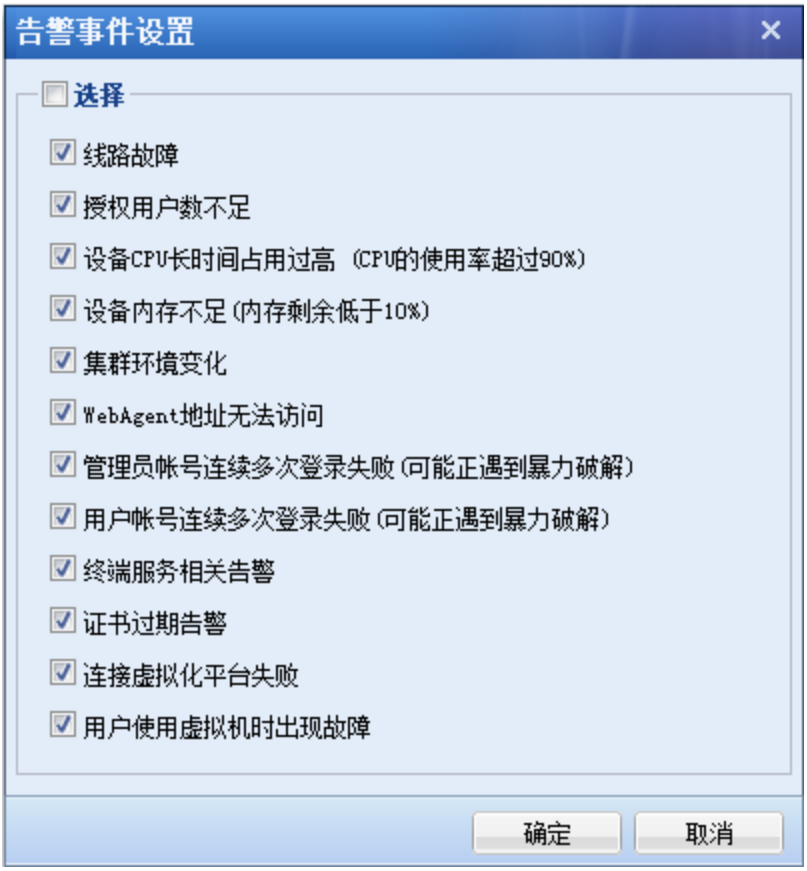
点击选择，则可以选择[选择当前页]，[选择所有页]，[取消选择]，显示如下：

[选择当前页]，则将该页的日志全部选上，

[选择所有页]，则将所有的日志选上，

[取消选择]，则将之前选择的日志取消掉。

点击告警事件设置后，可以选择相应的告警信息，显示如下：



『线路故障』当外网线路出现问题时会给指定的邮箱发送邮件告警；

『授权用户数不足』登录用户达到用户授权数时，会给指定的邮箱发送邮件告警；

『设备 CPU 长时间占用过高』设备 CPU 长时间过高，120 秒内，平均使用率超过 90%，会给指定的邮箱发送邮件告警，当设备恢复正常也会发送一封邮件；

『设备内存不足』当设备内存不足时，持续 4 分钟，内存低于 10%，会给指定的邮箱发送邮件告警，当恢复正常后，也会发送一份邮件通知设备恢复了；

『集群环境变化』当集群分发器发生变化时，会给指定的邮箱发送邮件告警；

『WebAgent 地址无法访问』：当 WebAgent 地址无法访问时，会给指定的邮箱发送邮件告警；

『管理员账号连续多次登录失败』管理员账号连续多次登录失败时，会给指定的邮箱发送邮件告警；

『用户账号连续多次登录失败』VDI 用户账号连续多次登录失败，会给指定的邮箱发送邮件告警；

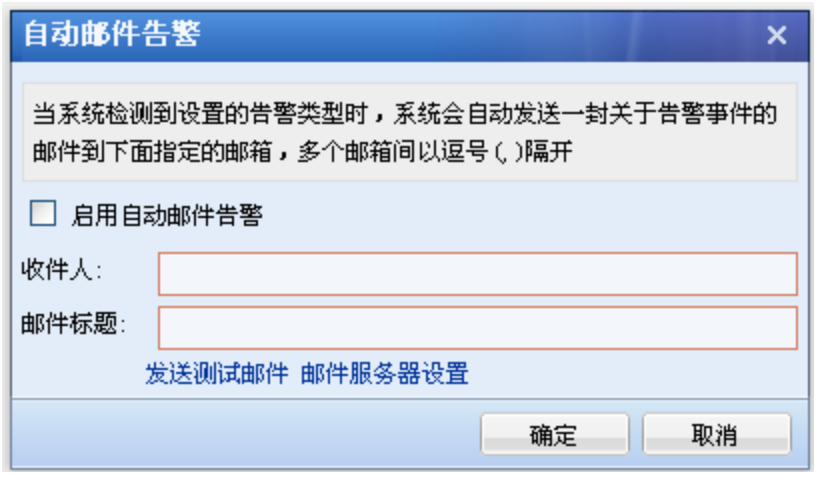
『终端服务相关告警』远程应用发布相关告警即当应用发布出现问题时，会给指定的邮箱发送邮件告警；

『证书过期告警』VDI 所使用到的 SSL 证书过期时，会给指定的邮箱发送邮件告警；

『连接虚拟化平台失败』VDC 连接到虚拟化平台时发生故障，会给指定的邮箱发送邮件告警；

『用户使用虚拟机时出现故障』用户接入使用虚拟机时发生故障，会给指定的邮箱发送邮件告警；

点击自动邮件告警后，可以勾选[启用自动邮件告警]并设置接收告警的邮件地址和邮件标题。设备会根据设置将告警邮件发送至设置的邮箱，页面显示如下：



点击发送测试邮件，设备会自动发送一封测试邮件给收件人。

点击邮件服务器设置，即链接到『邮件服务器』设置页面，详见 3.1.5 章节。

2.2.4. 终端服务

在『终端服务』中可以查看提供 VDI 服务的服务器的相应信息和状态。

WEBUI 路径：『运行状态』→『VDI 运行状态』→『终端服务』。

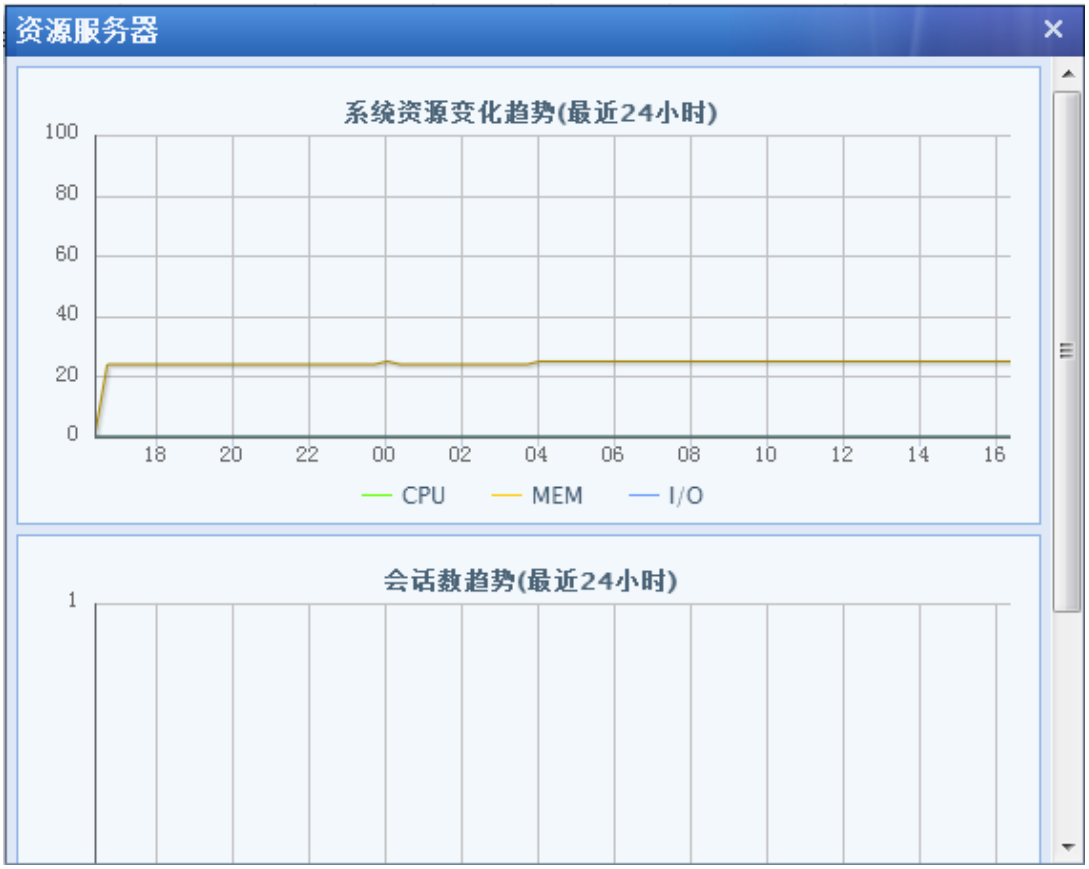
在这里可以看到 VDI 资源服务器和存储服务器的状态信息，包括服务器名称，服务器地址，服务器类型，CPU，内存，磁盘 I/O，远程应用会话，服务器会话及状态等信息。界面如下图所示：

『视图』选择需要查看的状态类型，包括[服务器状态]和[应用程序连接状态]，显示如下：

[服务器状态]显示的是在『VDI 配置』中『服务器管理』里面建立的服务器信息，显示其当前状态，如下图：

点击相应的服务器名称，能够查看该服务器上用户的使用情况，显示如下：

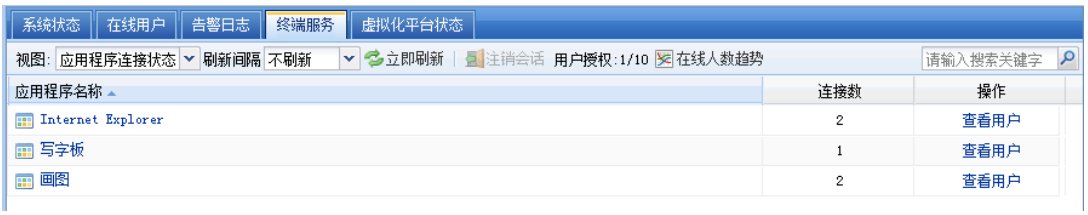
在资源服务器中，点击运行状态下的查看，可以查看该服务器的峰值记录，如下图：



在存储服务器中，点击运行状态下的查看，可查看该服务器最近 24 小时的系统资源变化情况，如下图：

勾选相应的用户，点击注销会话，则将用户访问该服务器的会话注销。

[应用程序连接状态]显示的是在『VDI 配置』中『服务器管理』里面启用了的服务并且在资源里面调用后的使用情况，显示如下：



点击相应的应用程序名称或查看用户能够查看该应用程序的用户使用情况，显示如下：

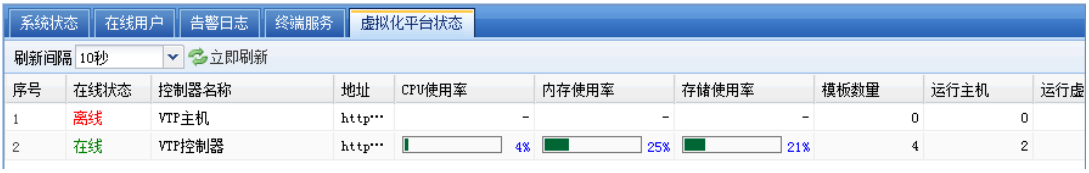
勾选相应的用户，点击注销会话，则将用户使用该应用程序的会话注销。

2.2.5. 虚拟化平台状态

在『虚拟化平台状态』中可以查看提供虚拟桌面服务的虚拟化平台的运行状态。

WEBUI 路径：『运行状态』→『VDI 运行状态』→『虚拟化平台状态』。

在这里可以看到虚拟化管理平台的控制器状态信息，包括控制器名称，地址，CPU 使用率，内存使用率，磁盘使用率，模板数量，运行主机和运行虚拟机等信息。界面如下图所示：



将鼠标指针停留在使用率显示图上，会详细显示当前使用率的具体信息，如下图：

第3章 系统设置

『系统设置』包含『系统配置』、『网络配置』、『接入选项』、『登录策略』、『传输优化』、『时间计划』，『管理员账号』『集群部署』等八个模块。如下图：

3.1. 系统配置

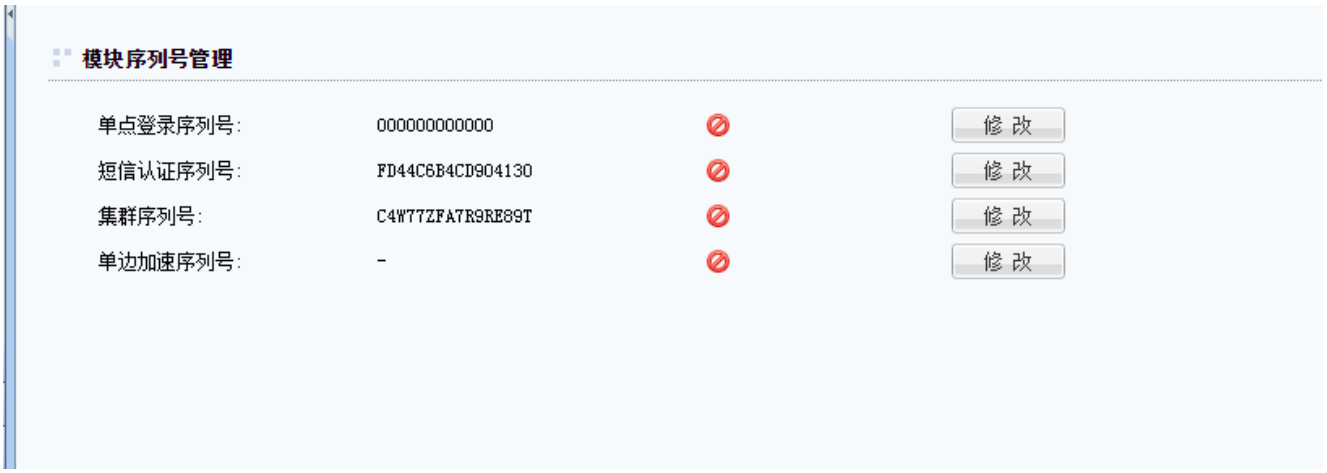
『系统配置』里面包含了『序列号管理』，『日期与时间』，『控制台配置』，『设备证书』，『邮件服务器』，『Syslog』，『SNMP』的设置，如下图：

3.1.1. 序列号管理

『序列号管理』分为『设备序列号管理』和『模块序列号管理』。

WEBUI 路径：『系统设置』→『系统配置』→『序列号管理』。

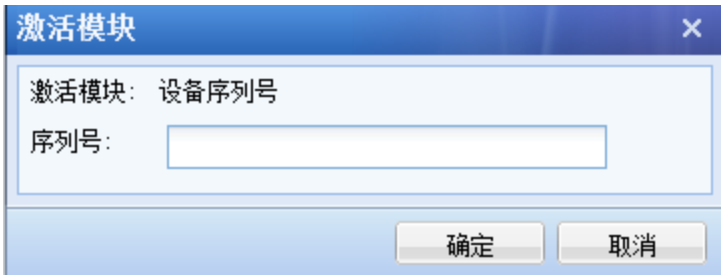
显示界面如下图：



『设备序列号管理』用于填写 VDC 设备的序列号，该序列号控制硬件网关的可用外网线路数量、VDI 用户的授权数，以及软件版本升级授权。不同的序列号对应着不同线路数量和接入用户数量，填入序列号时，这些授权数会自动生成。

『模块序列号管理』用于填写 VDC 设备扩展功能的序列号，正确填写序列号后，相应模块的功能就开启了，可以填写的序列号有单点登录序列号、短信认证序列号、集群序列号、单边加速序列号。

点击相应模块后的修改可修改序列号。界面如下图所示：



3.1.2. 日期与时间

『日期与时间』用于设定 VDC 设备的系统时间。

WEBUI 路径：『系统设置』→『系统配置』→『日期与时间』。

界面如下图所示：

在日期和时间后面可以自己设置相应的时间，点击保存则将新的设置在设备系统中保存，点击获取本地时间则是将设备的时间和登录设备的电脑时间同步，然后再点击保存，使配置生效。

勾选『自动与时间服务器同步』，选择指定的时间服务器，点击立即更新则设备的时间将会从指定的时间同步服务器上同步过来。

点击取消，取消当前修改。

注意：修改时间后会重启设备的所有服务！

3.1.3. 控制台配置

『控制台配置』用于设置设备的名称、控制台访问的端口、控制台超时时间以及是否允许远程维护。

WEBUI 路径：『系统设置』→『系统配置』→『控制台配置』。

界面如下图所示：

『设备名称』设备在集群时，用于分辨各设备的标识。

『https 端口』登录设备控制台的 https 端口，默认为 4430。

『http 端口』登录设备控制台的 http 端口，默认为 1000。勾选后，可通过 http 的 1000 端口登录设备控制台。

『超时时间』登录控制台后，在规定的时间内没有对控制台进行操作，即登陆超时，再操作时，需要重新登陆。

『远程维护支持』启用或禁用从外网口对设备控制台进行管理。

点击保存，保存当前修改。

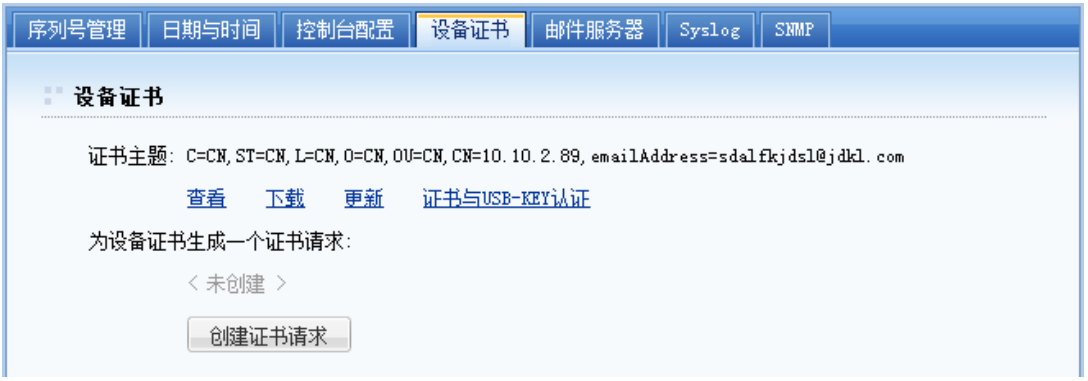
点击取消，取消当前修改。

3.1.4. 设备证书

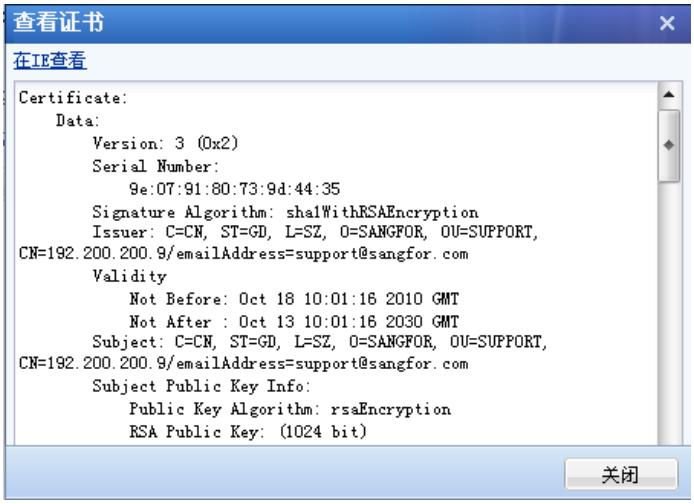
『设备证书』用于配置设备的证书，证书将用于客户端与设备建立 SSL 会话。

WEBUI 路径：『系统设置』→『系统配置』→『设备证书』。

界面如下图所示：



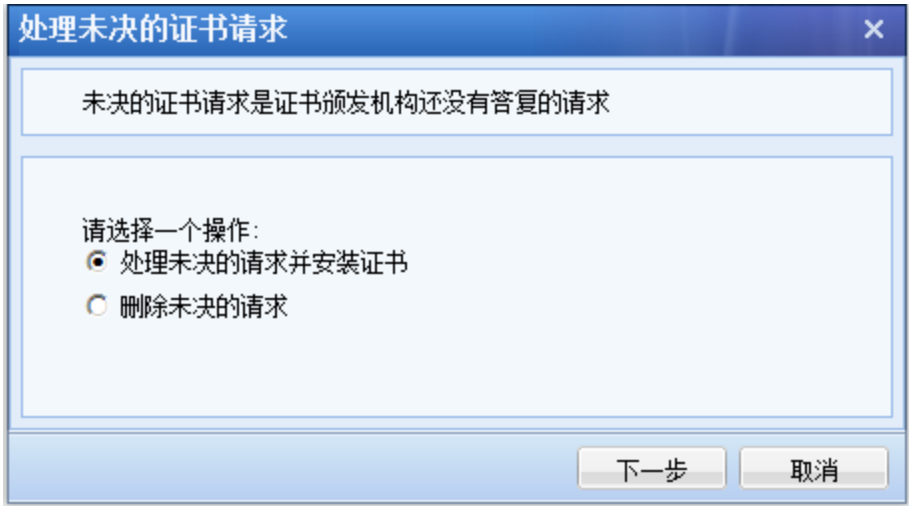
点击查看则可以查看设备当前的证书，显示如下：



点击下载则可以把设备证书下载下来。点击更新，则可以重新导入新的设备证书，将之前的设备证书替换掉。点击证书与 USB-KEY 认证，则会跳转到 4.7.1.4 章节里面的证书与 USB-KSY 认证，进行设置，后续章节将对此详细介绍。

在[为设备生成一个证书请求]下点击下载，即新生成一个证书请求，选择证书保存路径保存证书。显示如下：

点击处理未决的证书请求，可安装证书或删除未决的证书请求。



若选择[处理未决的请求并安装证书]，点击下一步，需选择需要安装的证书，如下图：

点击浏览，选择证书，并点击完成，即完成证书安装。

注：这里安装的证书格式类型只支持*.crt 或*.cer。

3.1.5. 邮件服务器

『邮件服务器』主要针对设备的 SMTP 服务器的设置，使设备能够对外发送相关的告警邮件。

WEBUI 路径：『系统设置』→『系统配置』→『邮件服务器』。

界面如下图所示：

『SMTP 服务器地址』填写相应 SMTP 服务器地址，例如 QQ 邮箱的服务器地址为 smtp.qq.com；

『端口号』设置 SMTP 服务器提供服务的端口号；

『身份验证』SMTP 服务器是否需要身份验证，若需要，这在勾上此选项并且填上相应的用户名密码；若不需要，可不勾选。

点击发送测试邮件，可以测试 SMTP 服务器是否正常，设备上面设置是否正确。

3.1.6. Syslog

『Syslog』用于将日志信息同步到 Syslog 服务器上。

WEBUI 路径：『系统设置』→『系统配置』→『Syslog』。

3.1.7. SNMP

『SNMP』用于与客户的 SNMP 管理软件或 SNMP 服务器通讯，通过 SNMP 协议管理设备内存信息等。

WEBUI 路径：『系统设置』→『系统配置』→『SNMP』。

3.2. 网络配置

『网络配置』包括『部署模式』、『多线路』、『路由设置』、『HOSTS』四个部分。如下图：

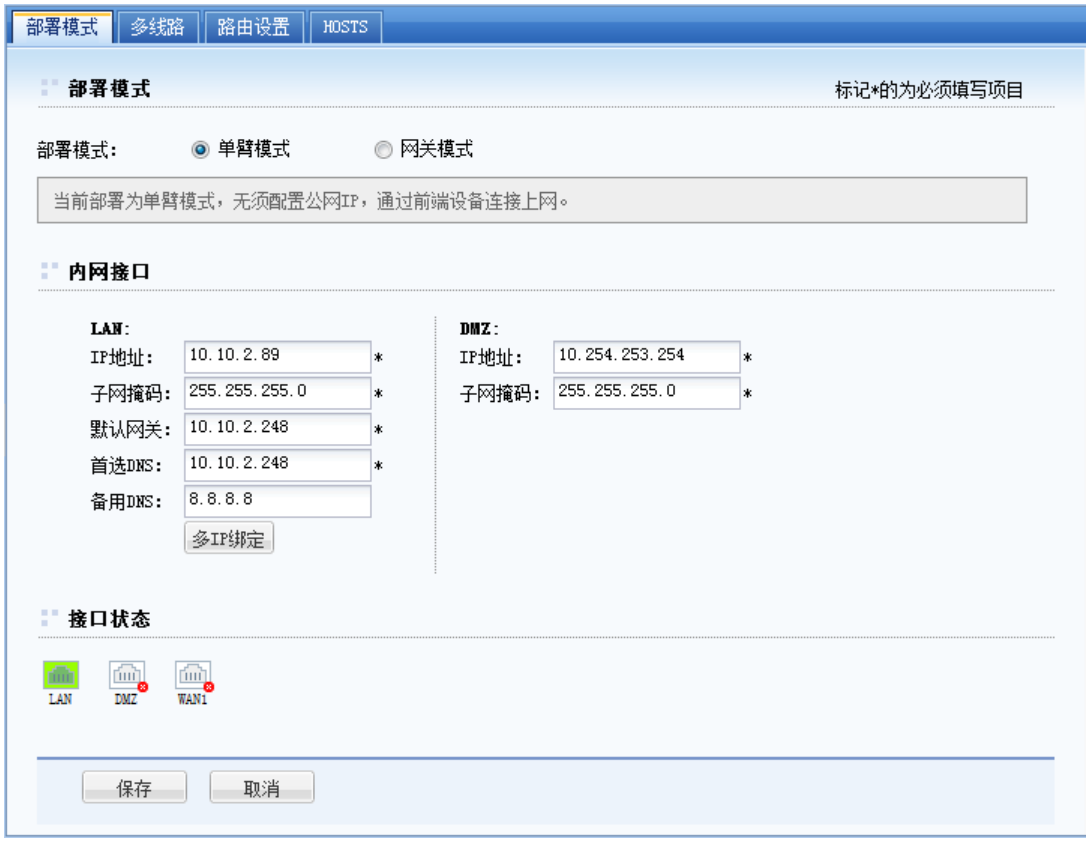
3.2.1. 部署模式

部署模式中有两种工作模式可供选择：单臂模式和网关模式。

WEBUI 路径：『系统设置』→『网络配置』→『部署模式』。

界面如下图所示：

选择单臂模式时，需要配置内网接口（LAN 口）IP 地址、子网掩码，默认网关，配置 DMZ 口 IP 地址、子网掩码，配置 DNS。页面如下：



选择网关模式时，不仅需要配置内网接口，同时也必须配置相应的外网线路。页面如下：

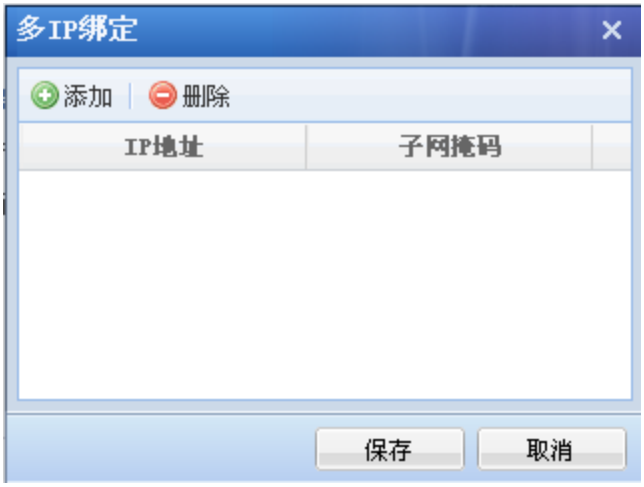
『内网接口』按照实际情况设置相应的地址和子网掩码；

在『外网接口』中，点击相应的线路名称，进入到该线路的编辑页面，显示如下：

勾起[启用该线路]即开启该线路，选择线路类型，可选择[以太网]或[ADSL 拨号连接]。

当选择[以太网]时，可以选择[自动获得 IP 地址和 DNS 服务器]，或者手动配置 IP 地址和 DNS 服务器地址，如果自动获取，则设备会从 DHCP 服务器获取相应的 IP 和 DNS 服务器地址。若选择手动配置，那需要配置相应的 IP，掩码，网关和该链路的 DNS 服务器地址。

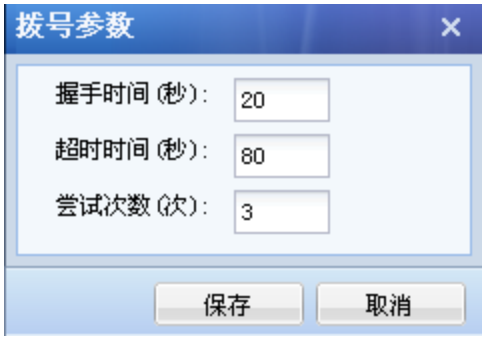
多 IP 绑定，外网接口为以太网模式下可以启用，在设备外网接口有多个 IP 时，点击多 IP 绑定按钮，出现以下对话框，点击添加，即可为 WAN 口绑定多个 IP，点击删除，则将之前绑定的 IP 删除。页面如下：



注意：网关模式部署时 LAN 口，DMZ 口和 WAN 口的地址不能在同一网段。

当外网线路为 ADSL 拨号时，需在『ADSL 拨号设置』中填写『用户名』和『密码』等信息，勾上[自动连接]，配置完毕点保存保存设置，设备将重启所有服务，重新登录后点击连接，则以后设备再断线后就可以"自动重拨"了。当拨号出现问题的时候可以点击查看详情，查看相应拨号信息。页面如下：

点击拨号参数可以设置拨号基本参数，一般保持默认即可。显示如下：



3.2.2. 多线路

『多线路』，在使用多条 WAN 口线路或者需要在单臂模式下启用多线路功能时，都需要在此处添加“多条线路”，这里可以对线路的信息进行增删和修改。

WEBUI 路径：『系统设置』→『网络配置』→『多线路』。界面如下图所示：

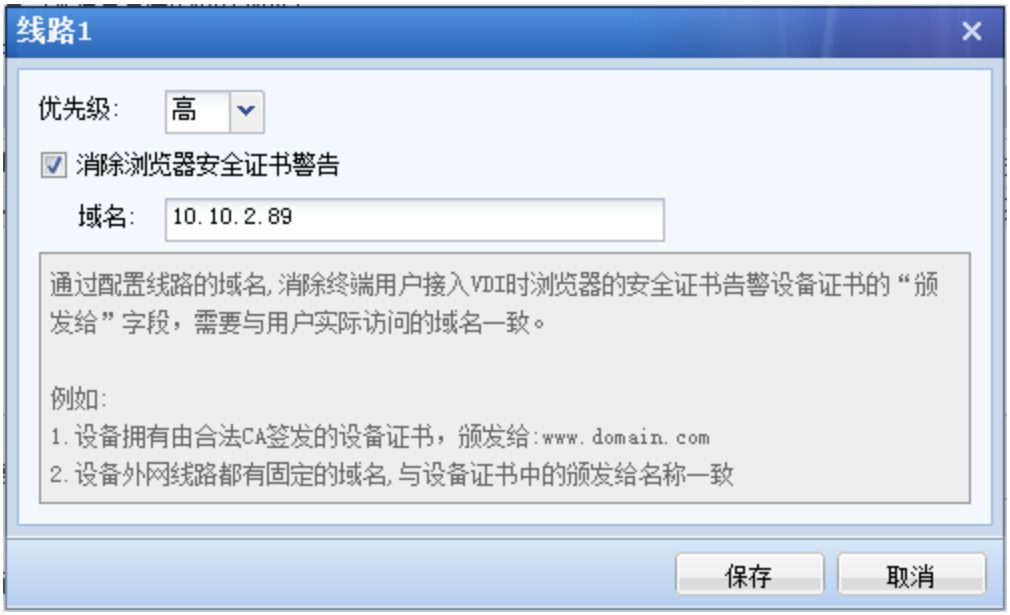
上图为“单臂模式”配置页面。

上图为“网关模式”配置页面。

『多线路传输』可配置 VDI 多线路功能。在有多条外网线路，且 VDI 接入也需要使用多线路时，则可以启用该功能来提升 VDI 的传输速度和接入稳定性。

勾选[启用多线路]，即开启 VDI 多线路选路功能。启用多线路后，用户登录 VDI 时，将会自动探测，并选择最快的线路接入。VDI 多线路接入方式有两种，一种是 VDC 设备网关模式部署，直接连公网，VDI 用户通过设备的公网地址直接接入。另一种是 VDC 设备放在内网，前面还有其它的网关，VDI 用户通过前置设备接入，需要在前端设备中将外网地址映射给我们 VDC 设备，显示如下：

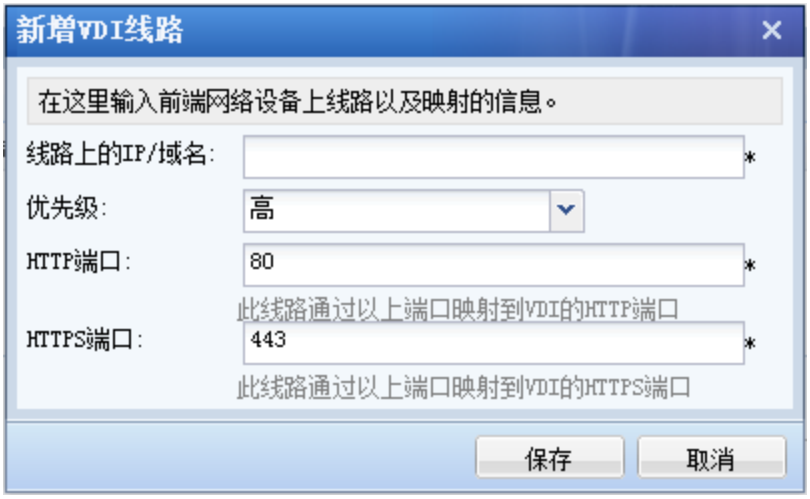
点击设置，设置线路优先级以及支持配置域名消除终端用户接入 VDI 时弹出证书告警框，界面如下：



勾选[消除浏览器安全证书告警]，填写相应线路域名，即可设置终端用户接入 VDI 时，不弹出设备证书告警框。

若选择[VDI 用户通过前置设备接入]，需要添加线路，如下图：

点击新增，设置线路的 IP/域名，选择优先级和 VDI 接入的端口，如下图：



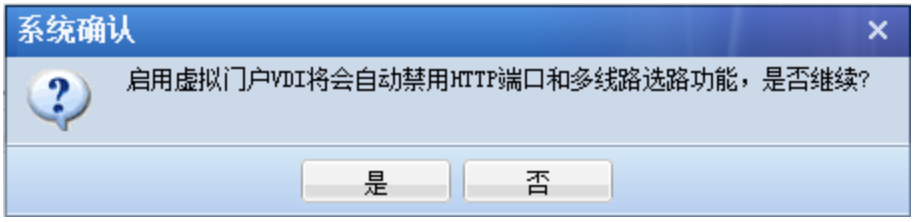
『线路上的 IP/域名』设置的是外网链路的 IP 地址或者域名，

『优先级』设置该链路的等级，优先级高的链路优先被选。

『HTTP 端口』填写前置设备映射给 VDC 设备的 HTTP 端口。

『HTTPS 端口』填写前置设备映射给 VDC 设备的 HTTPS 端口。

当设备在『系统配置』→『VDI 选项』→『登陆策略』选择虚拟门户时，将禁用 VDI 多线路功能，VDI 多线路传输将无法启用，提示如下：



『多线路-上网数据选择策略』指当 VDC 设备以网关模式部署，内网用户上网也需要使用多线路选路。用户上网的选路策略分为以下四种，如下图：

[按每条线路的剩余下行带宽优先选择线路]，系统自动根据每条线路的剩余带宽（下行带宽）自动选择剩余带宽较大的线路，充分利用剩余带宽；

[按每条线路的剩余上行带宽优先选择线路]，系统自动根据每条线路的剩余带宽（上行带宽）自动选择剩余带宽较大的线路，充分利用剩余带宽；

[平均分配所有连接到每条线路]，系统把所有的连接平均分配到每条线路，此时不考虑每条线路的剩余带宽；

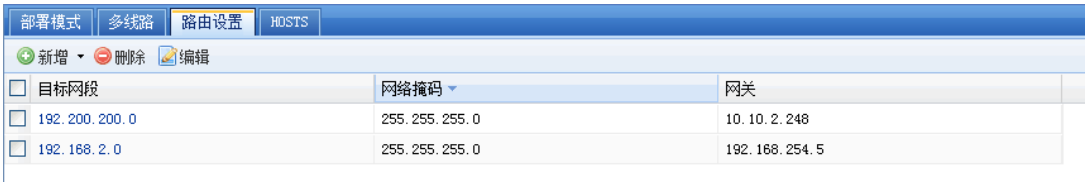
[优先选择前面的线路（有利于 VPN 部署）]，默认使用最先启用并且是有效的线路，当该线路断线或者不可用时，自动切换到下一条可以使用的线路；

3.2.3. 路由设置

对需要 VDC 设备网关转发的数据（VPN 或非 VPN）及 VDC 设备本身需要转发的数据进行的路由。『路由设置』主要用于实现两种功能：1、代理多网段上网时添加回包路由。2、访问 VPN 内部多子网时需要设置路由。

WEBUI 路径：『系统设置』→『网络配置』→『路由设置』。

界面如下图所示：



点击新增，选择[新增路由]和[批量新增路由]，显示如下：

选择[新增路由]，可添加一条路由，如下图：

[目标网段]路由指向的目标地址段。

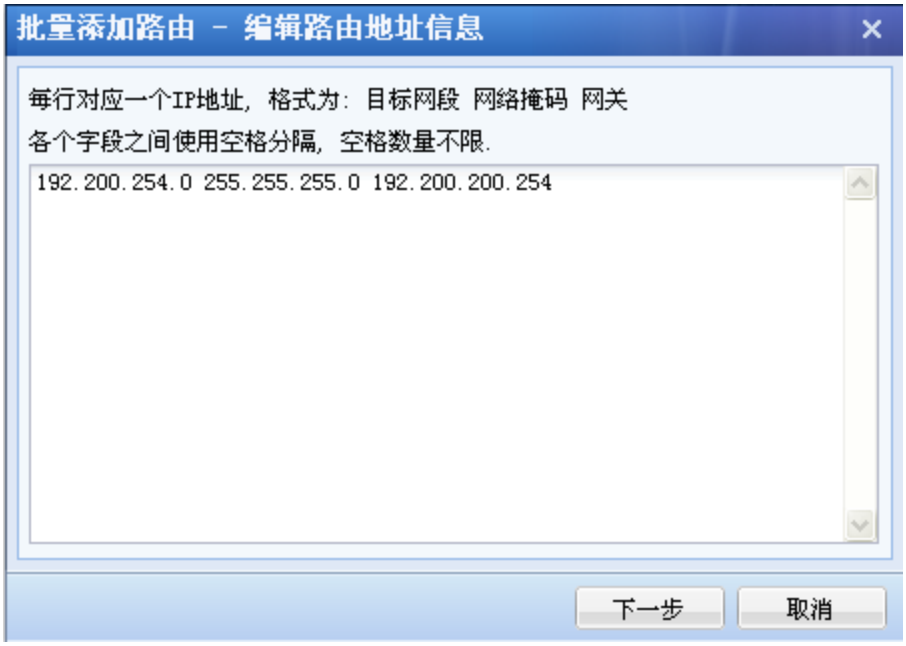
[网络掩码]目标地址段的子网掩码。

[网关]到达目标地址段的下一跳地址。

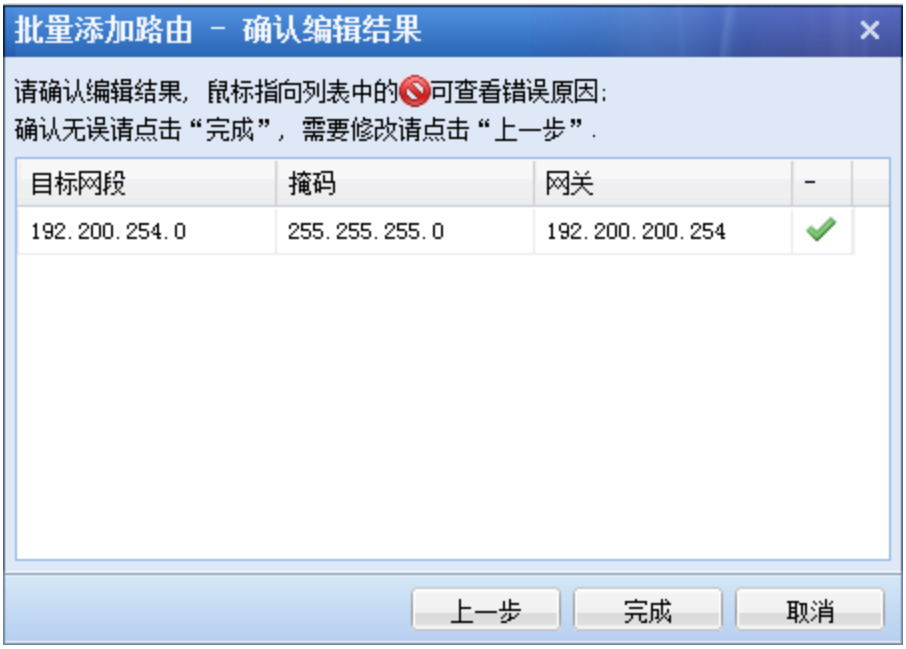
点击保存并继续添加，可继续添加路由。

点击保存，即保存配置。

选择[批量添加路由]，可一次性添加多条路由，如下图：



点击下一步，确认路由信息是否正确，若正确，点击完成，保存配置。如下图：

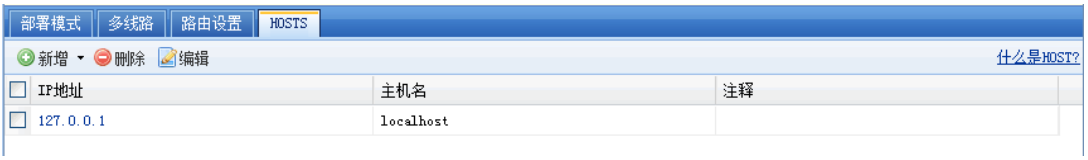


3.2.4. HOSTS

『HOSTS』用于定义 VDC 设备设备内置的 host 表，以解决 VDI 用户需要通过域名或机器名来访问内网资源的问题，常用于 VDC 设备内网有“域”的情况下。这里可以定义“域名”或“机器名”所对应的“host 主机 IP”。

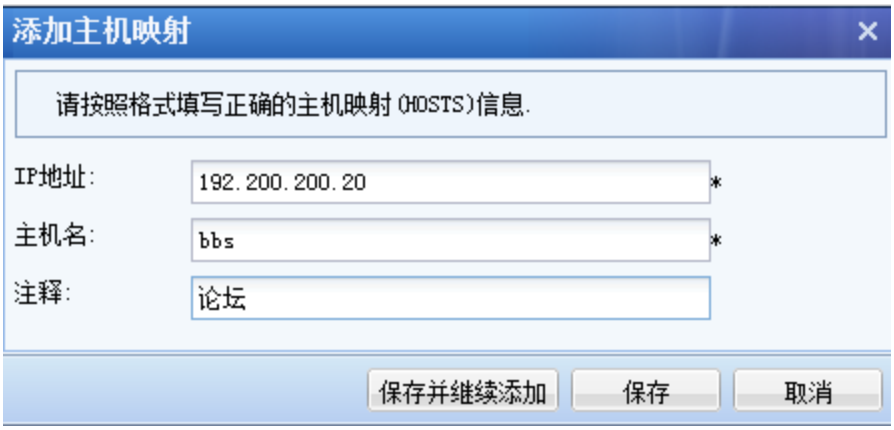
WEBUI 路径：『系统设置』→『网络配置』→『HOSTS』。

界面如下图所示：



点新增按钮可选择[新增主机映射]或[批量新增主机映射]。显示如下：

选择[新增主机映射]，弹出【添加主机映射】对话框，如下图所示：

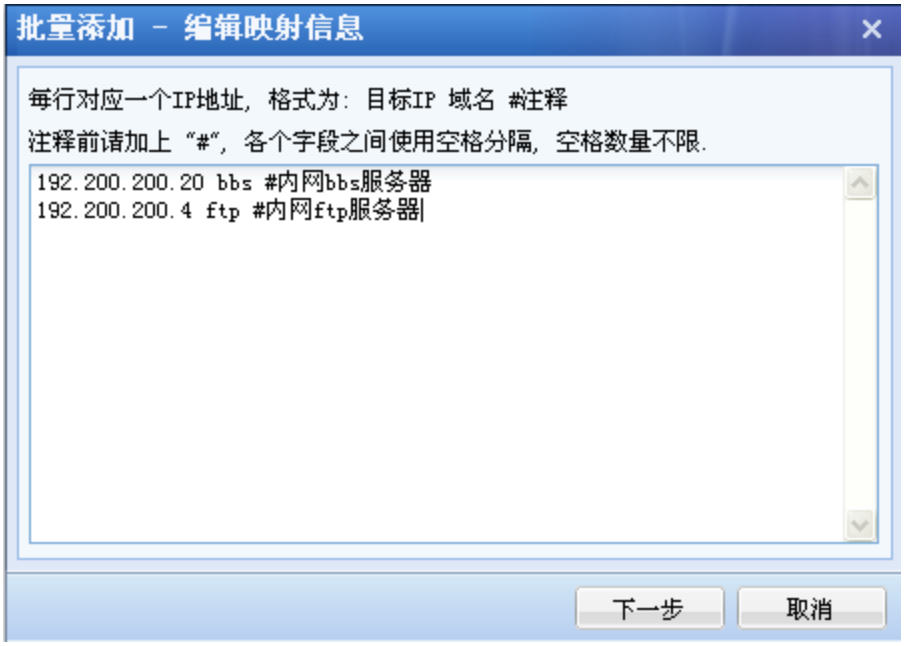


『IP 地址』需要添加映射的 IP 地址。

『主机名』该 IP 对应的主机名称。

『注释』对该 IP 地址对应主机地址的注释。

HOSTS 也可以批量设置，选择[批量新增主机映射]，格式如下：



3.3. 接入选项

『接入选项』包括客户机、VDI Client、内网域名解析、单点登录设置、第三方设备等五个选项。

如下图所示：

3.3.1. 客户机

客户机设置选项包括『客户机默认权限』、『个性化设置』、『客户机清理』等三个选项。

WEBUI 路径：『系统设置』→『接入选项』→『客户机』。

『客户机默认权限』可配置客户机显示桌面、安装应用、新客户机接入的默认动作。

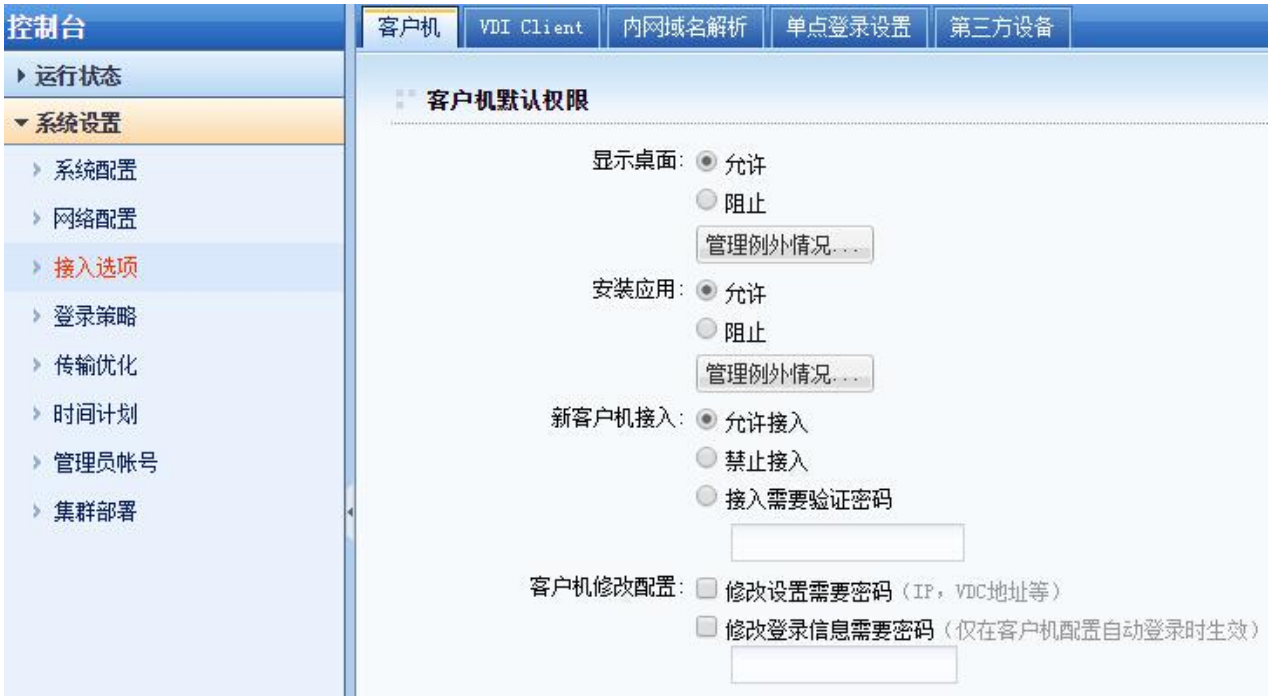
如果勾选允许“显示桌面”，则新客户机接入时默认显示 VDI 桌面，点击管理例外，可以设置部分客户机使用相反的动作，即不显示 VDI 桌面。

如果勾选允许“安装应用”，则客户机接入后可以安装自定义应用，点击管理例外，可以设置部分客户机使用相反的动作，即不允许自行安装应用。

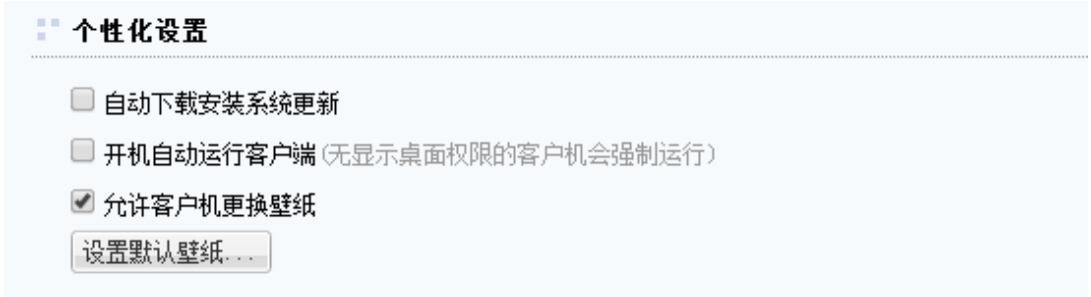
如果在“新客户机接入”勾选为允许接入，则新客户机可以直接接入 VDC 设备。或者通过勾选接入需要验证密码，则新客户机接入时需要输入所设置的密码才能接入。

如果勾选修改配置需要密码，则可以防止终端用户随意修改瘦客户机配置。

如果勾选修改登录信息需要密码，可以终端用户随意修改瘦客户机登录信息。

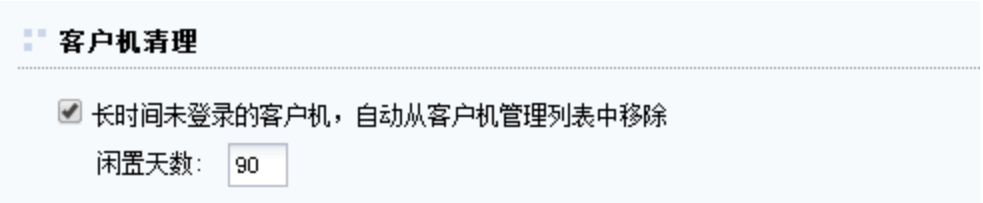


『个性化设置』包括自动下载安装系统更新、开机运行客户端、允许客户机更换壁纸等选项。



点击设置默认壁纸，可以设置客户机接入后使用的默认壁纸。

『客户机清理』设置将闲置一定时间的客户机自动从客户机列表中删除。



3.3.2. VDI Client

『VDC Client』用于设置客户机的功能模块的开启。

WEBUI 路径：『系统设置』→『接入选项』→『VDI Client』。

界面如下所示：

『用户访问入口』里设置 VDI 的服务监听端口。

『HTTPS 端口』设置 HTTPS 的监听端口，默认值为 TCP 443 端口。点击设置端口进行 HTTPS 监听端口设置，可设置多个端口。也可以手动输入多个端口，用逗号隔开。

[启用 HTTP 端口]设置 HTTP 的监听端口，默认值为 TCP 80 端口。当在『登录策略』中选择『虚拟门户』时，不能启用 HTTP 端口。

『客户端自定义』里设置 VDI 客户端接入选项。

『没有证书或只有一个证书的时候不弹出证书选择框』设置在使用证书登录的客户机上只有一个证书或无证书时的证书选择动作。

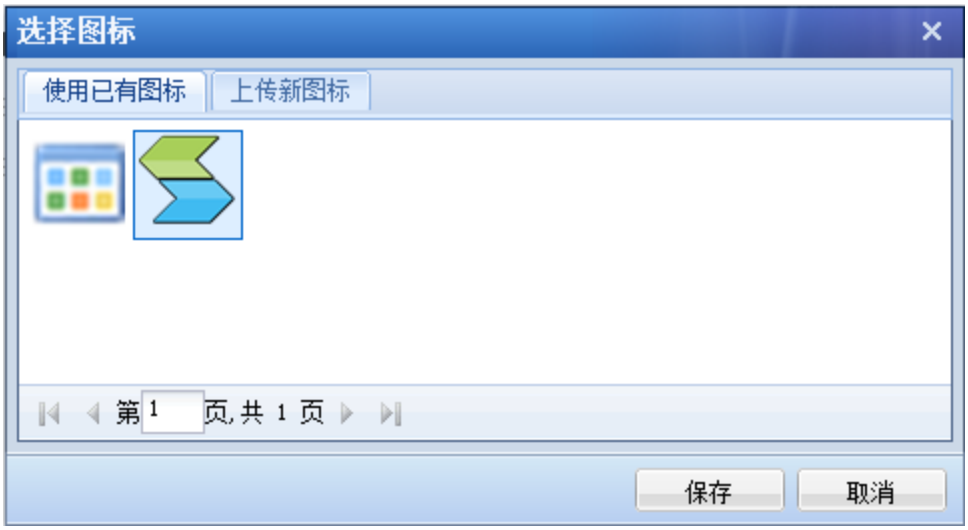
『断线自动重试连接』设置客户机断线后是否自动重连。启用"断线自动重试连接"，必须启用"允许用户选择自动登录"和"允许用户保存密码"。

『允许用户选择自动登录』设置客户机是否允许用户开机自动登录。启用"允许用户选择自动登录"，必须启用"允许用户保存密码"。

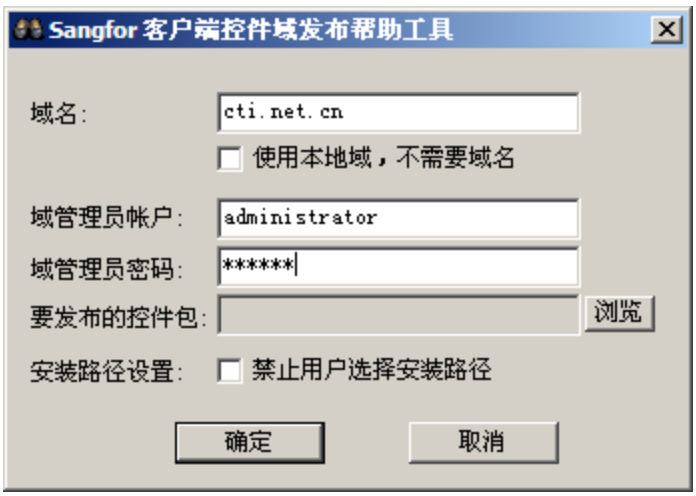
『允许用户保存密码』设置客户机是否允许保存用户密码。

『显示客户端组件的下载链接』设置是否在 VDI 登录界面上显示下载链接。

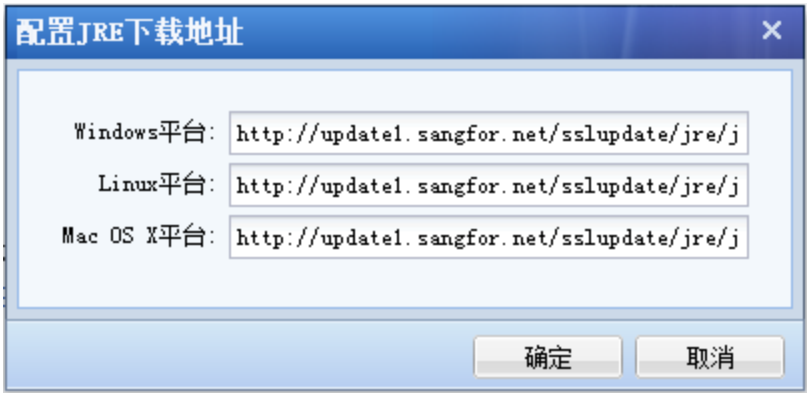
『自定义登录客户端的快捷方式图标』设置客户端程序安装后的程序图标。可以选择使用已有图标，或者上传新图标。



客户端组件使用微软 AD 域下发安装时，需下载 AD 域配置工具和客户端组件安装包，点击 AD 域配置程序和客户端组件安装包，即可下载。域下发帮助工具配置界面如下：



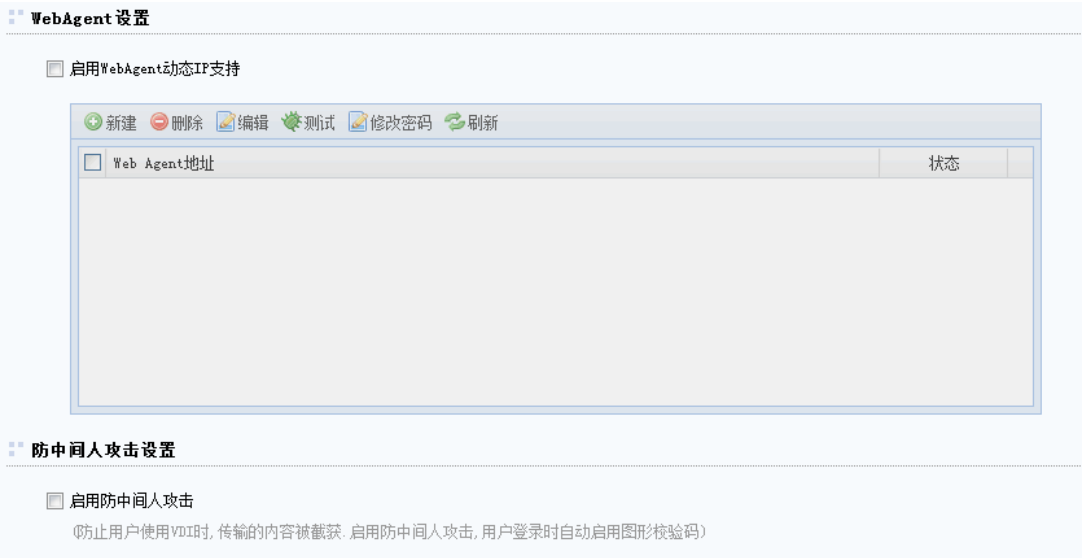
在非 IE 浏览器下，用户访资源时，需要下载并安装 JRE，点击配置 JRE 下载地址，弹出编辑框，如图所示：



在『Windows 平台』、『Linux 平台』和『Mac OS X 平台』后面的输入地址，非 IE 浏览器登陆 VDI 时，根据此地址下载 JRE 安装包。

『Webagent 设置』当设备在没有固定公网 IP 的情况下，需要建立连接，必须使用 WebAgent 动态寻址。

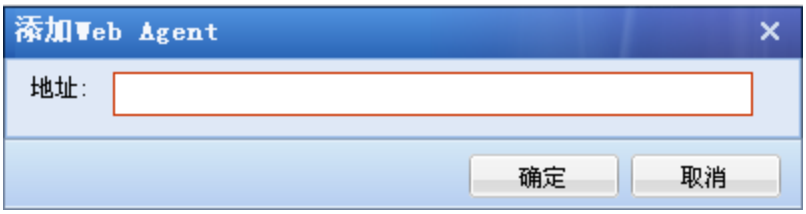
勾选『启用 WebAgent 动态 IP 支持』，即启用 WebAgent 动态寻址功能。可以在这里新增/删或修改 WebAgent，如下图所示：



『Webgent 地址』用于显示 Webagent 地址。

『状态』显示当前 Webagent 的状态。

点击新建即可新增一条 Webagnet。点击后如下图：



在弹出的输入框中输入申请到的 Webagent 地址，点击确定。

勾选相应的 webagent 地址，点击测试，如果弹出如下框的提示，证明填写正确。

勾选相应的 Webagent 地址，点击删除或编辑可以进行删除或编辑 webagent 地址。

勾选相应的 Webagent 地址，点击修改密码可以设置 Webagent 网页的密码，以防止非法用户往 Webagent 网页更新虚假 IP 地址。

点击刷新，可以刷新 Webagent 的当前状态。

『防中间人攻击设置』用来防止通信的数据被非法用户篡改和窃取。

『启用防中间人攻击』勾选后，用户登录时强制启用图形校验码，并且会强制安装控件。配置界面如下图所示：

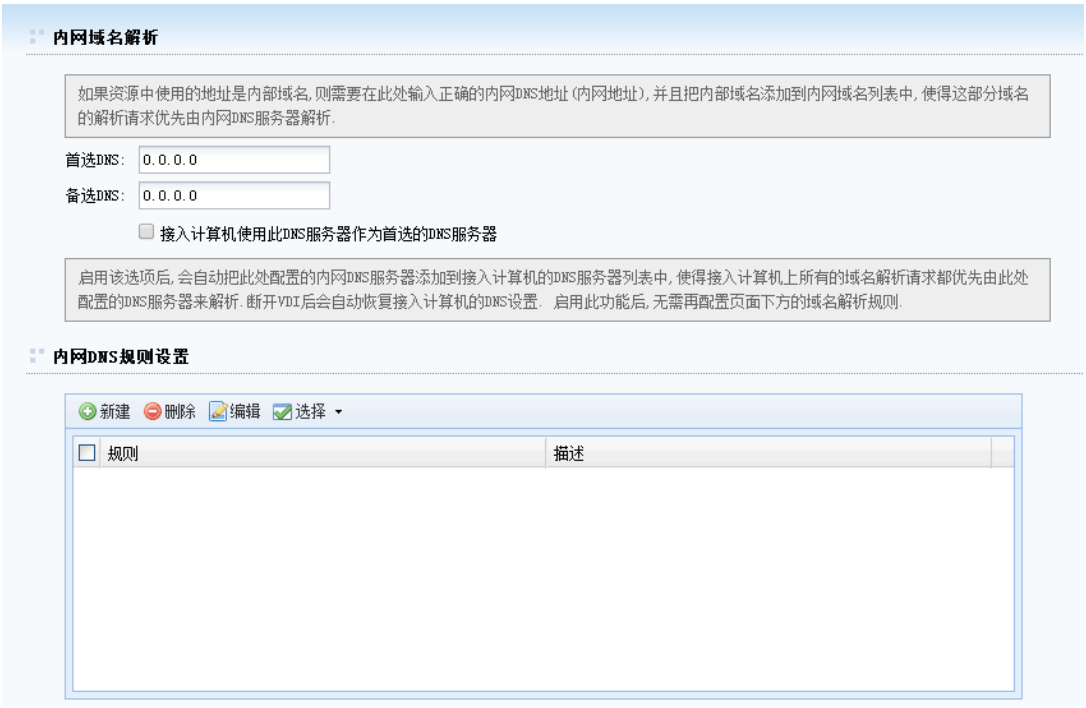
最后点击保存和配置生效。

3.3.3. 内网域名解析

VDC 设备支持通过内部域名访问资源应用。内网存在此类应用时，一般有一台或多台内网 DNS 服务器，给内网电脑提供内网域名解析服务。通过 VDC 设备需要访问此类应用时，可以通过『内网域名解析』配置来实现。

WEBUI 路径：『系统设置』→『接入选项』→『内网域名解析』。

界面如下所示：

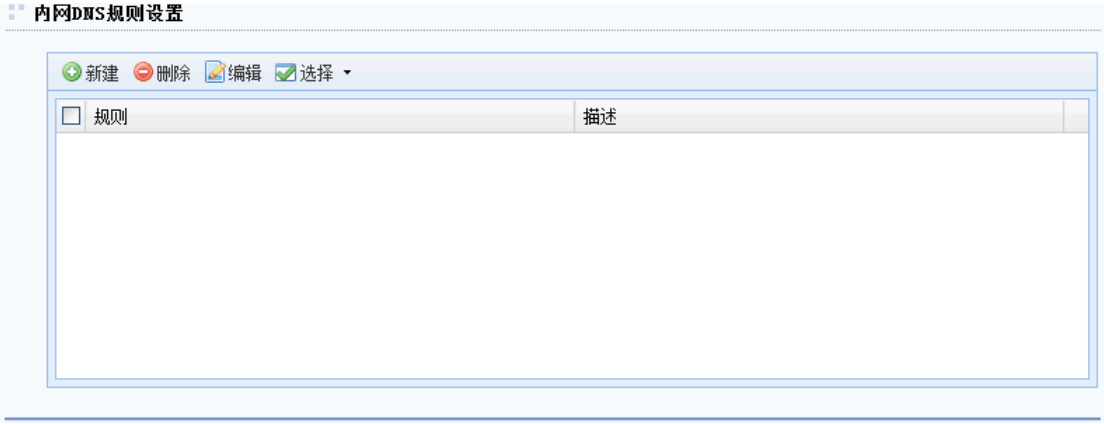


在『内网域名解析』中分别把内网 DNS 服务器的 IP 地址填写在『首选 DNS』和『备份 DNS』上，如果只有一台内网 DNS 服务器，则只需填写『首选 DNS』。然后在资源设置下填写资源主机地址或 URL 时以域名方式填写。客户端访问 VDI 的域名资源时，直接由『内网域名解析』中的 DNS 服务器进行解析。

[接入计算机使用此 DNS 服务器作为首选的 DNS 服务器]即将首选 DNS 和备选 DNS 的地址下发到登录 VDI 客户端的网卡中的主备 DNS 中。主要应用于当域控制器同时作为内网 DNS 服务器时，登录 VDI 客户端后访问的内网服务器需通过域控制器来认证的情况。

如果没有勾选[接入计算机使用此 DNS 服务器作为首选的 DNS 服务器]，且存在大量

的域名应用资源，在设置好『内网域名解析』后，可以进一步采用『内网 DNS 规则设置』处理，界面如下：



点击新建出现【新建域名解析规则】对话框：

『域名』在规则列表中需要访问的域名。

『描述』可随意填写便于理解记忆的文字。

点击确定保存配置。然后在填写资源主机地址或 URL 时以 IP 方式填写。客户端访问域名资源时，如果访问的域名符合在此定义的域名规则，将由设备内部的 HOST 表或『内网域名解析』中的 DNS 服务器进行解析，并将解析结果发送给客户端。

勾选相应的域名解析规则，点击删除或编辑，对选中的规则进行删除和编辑操作。点击选择选中所有规则或者取消所有选择。

1.如果资源中使用的地址是内部域名，且内网有专门的 DNS 服务器进行解析，推荐在此添加规则，使得这部分域名的解析请求优先由内网 DNS 服务器解析，否则不要在此添加任何规则！

2.此处添加的规则最多支持 100 条；不支持中文域名解析。

3.3.4. 单点登录设置

单点登录，也称为 SSO。就是通过用户的一次性认证登录，即可获得需访问系统和应用软件的授权。用户登录 VDI 以后，在使用配置好的单点登录应用程序时，不需要再次手动输入用户名和密码，能够自动完成用户名和密码的输入，并进行登录。管理员可以在『单点登录设置』页面来配置单点登录的服务。

WEBUI 路径：『系统设置』→『接入选项』→『单点登录设置』。

界面如下所示：

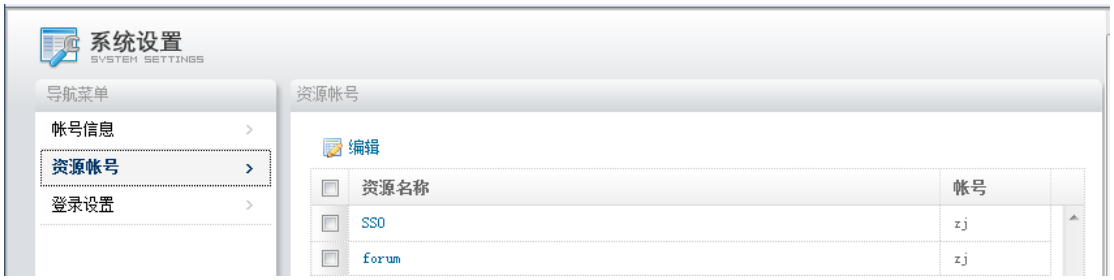
『单点登录设置』：勾选[启用]用户登录后可进行资源的单点登录，勾选『禁用』用户登录后不可进行资源的单点登录。

下载单点登配置助手点击即可下载单点登录配置助手。单点登录配置助手用于在使用自动填表方式时帮助管理员录制单点登录文件。

下载单点登配置文件点击即可下载单点登录配置文件。在设置好资源的单点登录方式后，需下载此文件使用单点登录配置助手来录制单点登录文件。

点击浏览，选择录制好的单点登录文件，然后再点击上传，将录制好的单点登录配置文件上传到设备中。

勾选[允许用户修改单点用户密码]，用户登录 VDI 后可以修改单点登录的用户名和密码。点击设置便可出现私人用户设置界面，左边列表中选择『资源账号』，页面如下：



勾选相关的资源，再点击编辑，弹出编辑框，如下图所示：

在【设置帐号】页面可以修改登录此资源的用户名和密码。点保存可以保存设置。

3.3.5. 第三方设备

可以让客户虚拟机开机后单点登录到 AC 上网行为管理设备进行审计（该功能同时需要到深信服上网行为管理设备中配置城市热点 IP 为 VDC IP）。

1.只有私有用户，并且关联了 SSO 资源，才能够在资源列表页面进行 SSO 配置。

3.4. 登录策略

『登录策略』可以用来针对不同的用户或用户组设置个性化的登录页面。

3.4.1. 登录策略

WEBUI 路径：『系统设置』→『登录策略』。

界面如下所示：

[所有用户都使用相同的登录页面]在此处可以针对所有用户使用的登录页面进行全局设置。

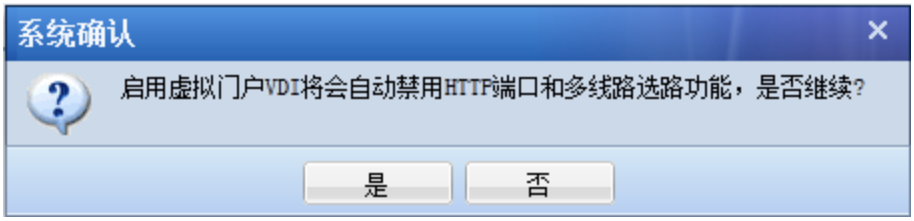
在[页面选择]中选择登陆页面，可选择使用系统自带模板或者用户自定义的模板。

点击查看缩略图可以看到当前可以使用的系统模板的缩略图。

界面如下所示：

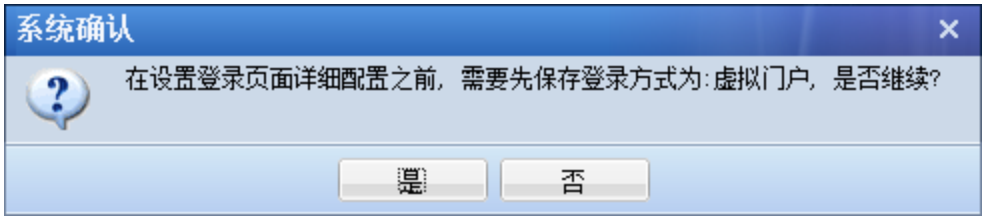
[虚拟门户]可设置允许不同的用户使用多个不同的登录风格及服务页面。

选择[虚拟门户]策略，VDI 的 HTTP 端口和多线路选路功能将不可用，会弹出如下提示：



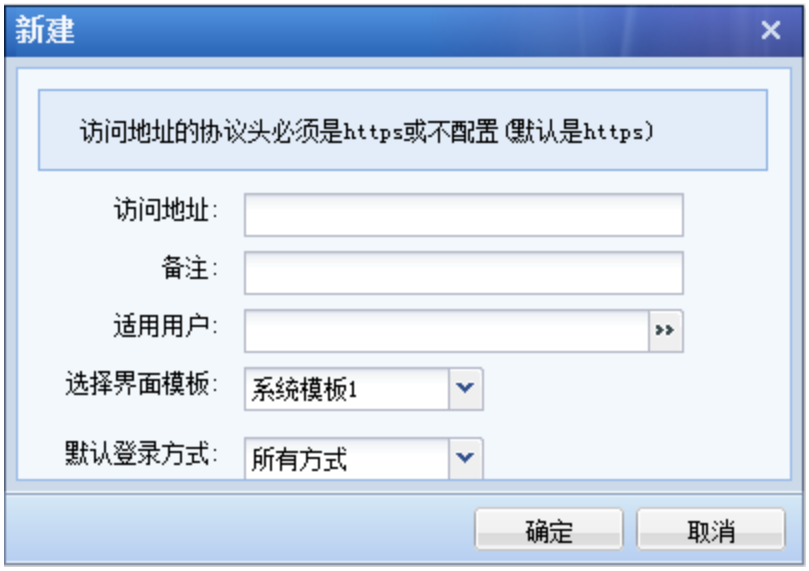
点击设置按钮，可以对『虚拟门户』进行详细设置。

界面如下所示：



点击是按钮，提交成功后，出现如下图所示的界面：

点击新建按钮，如下图所示：

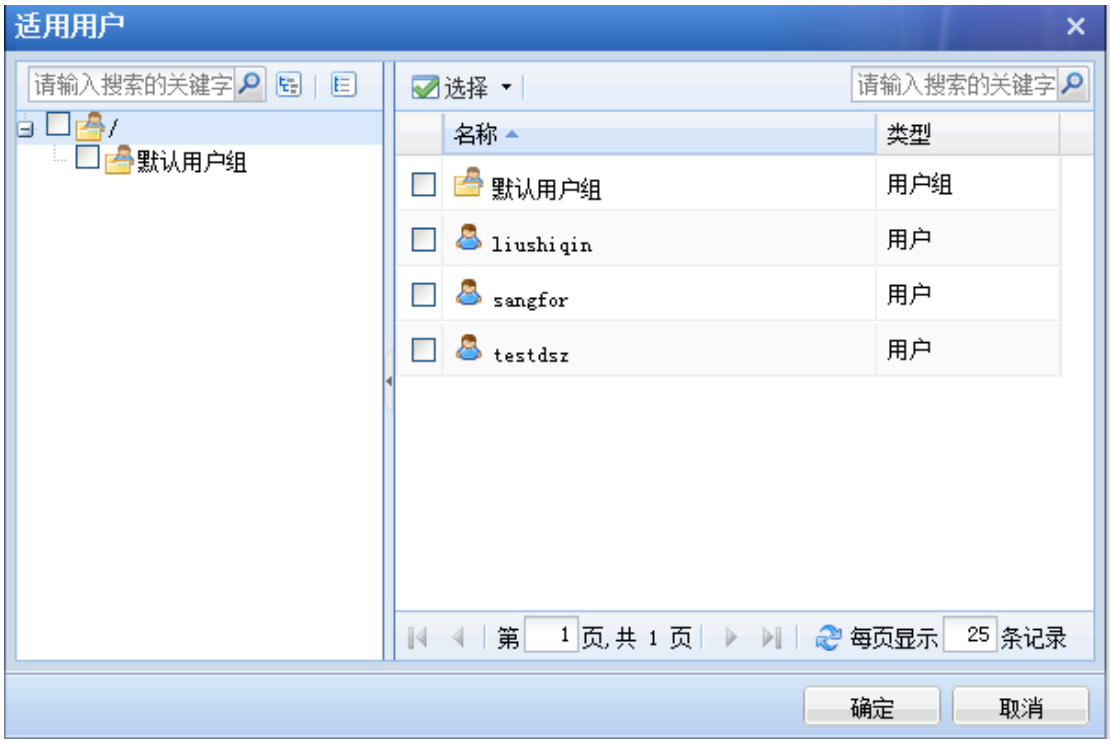


『访问地址』用来填写访问 VDI 登录页面的地址。该地址不能以 http://开头。

『备注』用户填写一些描述信息。

『适用用户』选择关联该条登录策略的用户或者用户组。

点击  图标，如下图所示：



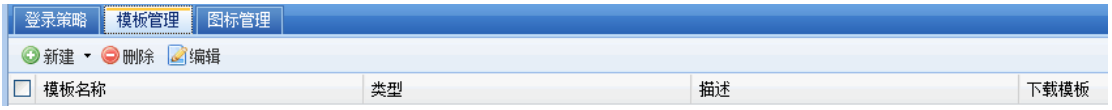
勾选关联的用户或者用户组，点击确定按钮，完成。

3.4.2. 模板管理

『模板管理』用来设置登录页面的模板，供用户选择使用。

WEBUI 路径：『系统设置』→『登录策略』→『模板管理』。

界面如下所示：



点击新建按钮，可以选择[以内置页面为模板新建]和[上传自定义页面]。如下图：

选择 [以内置页面为模板新建]就是以系统自带模板为基础来制作新的用户登录模板。

如下图所示：

『模板名称』用来自定义新建模板的名称。

『模板描述』用来添加新建模板的描述信息。

『模板选择』用来选择作为新建的模板的内置页面。

『页面标题』用来自定义新建模板显示的标题信息。

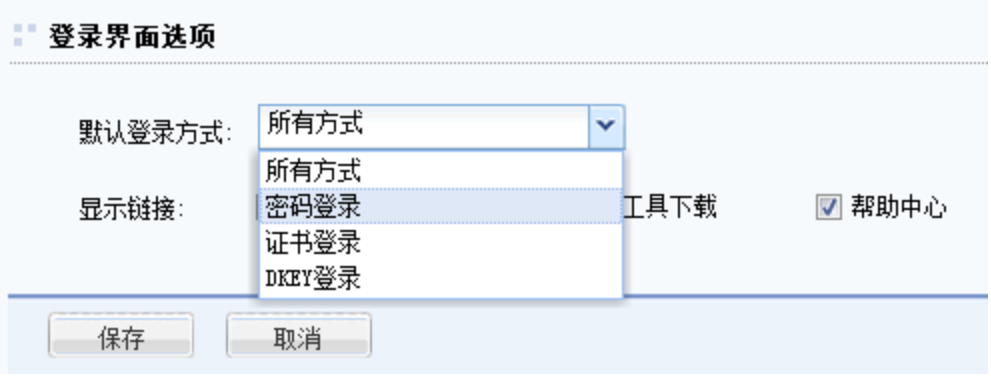
『当前 LOGO』显示当前登录模板的系统 LOGO，通过点击『上传 LOGO』自定义新的系统 LOGO，文件格式支持.png,.gif,.jpg,.bmp,图片最大高度是 48px,文件最大不超过 1MB。

『背景色』用来选择新建模板显示的背景颜色。

『公告信息』可以编写一些公告或者提示信息，支持 HTML，不能超过 1024 个字符。

『登录界面选项』包括默认登录方式设置，以及登录界面显示链接设置。默认登录方

式包括【所有方式】、【密码登录】、【证书登录】及【DKEY 登录】等。可选显示的链接包括【客户端组件下载】、【修复工具下载】、【帮助中心】等。



若系统启用了匿名登录，则无法选择默认登录方式。

点击保存按钮，新建模板设置成功。

选择『上传自定义页面』就是使用客户自己设计的登录页面。

界面如下所示：

『模板名称』用来自定义新建模板的名称。

『模板描述』用来添加新建模板的描述信息。

『模板文件』上传自定义的模板文件，模板文件包格式必须是 ZIP。

『页面标题』用来自定义新建模板显示的标题信息。

『公告信息』可以编写一些公告或者提示信息，支持 HTML，不能超过 1024 个字符。

点击『预览』可以看到预览效果图。

点击保存按钮，新建模板设置成功。

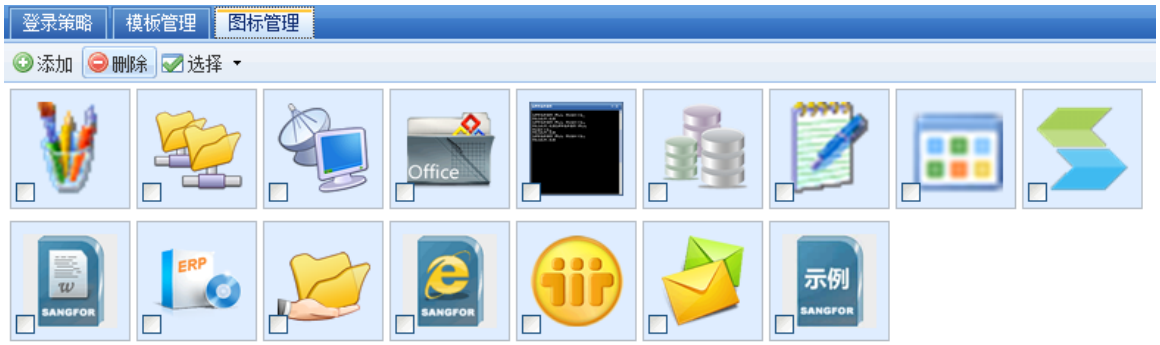
制作模版可以参考右边的示例，设备默认提供四种示例可供参考。

3.4.3. 图标管理

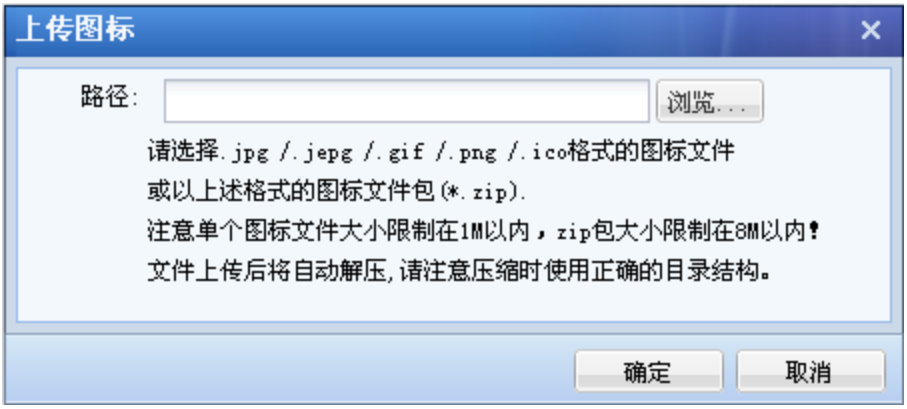
『图标管理』用来管理设备中用到的各种图标信息。

WEBUI 路径：『系统设置』→『登录策略』→『图标管理』。

界面如下所示：



点击添加按钮，可以上传新的图标，如下图所示：



勾选图标，点击删除按钮，可以删除选中的图标。

点击选择，可全部选中或取消选择。

3.5. 传输优化

本页面可配置 VDI 访问优化选项，优化 VDI 的访问速度。包括『远程应用优化』、『传输优化』和『Flash 重定向』等标签页。如下图所示：

3.5.1. 远程应用优化

WEBUI 路径：『系统设置』→『传输优化』→『远程应用优化』。

界面如下所示：

[有损压缩设置]启用该选项后，远程应用显示的图像会根据设置的质量等级进行压缩，以提高传输效率。

[图像缓存设置]启用该选项后，远程应用会对图像进行缓存，以提高图像滚动的刷新效果，启用该选项会增加服务器的 CPU 使用率。

[动态图像过滤]启用该选项后，对于远程应用中的 FLASH 动画等动态图像会进行过滤，以节省带宽，提高应用的访问速度。

3.5.2. 传输优化

WEBUI 路径：『系统设置』→『传输优化』→『传输优化』。

界面如下所示：

[启用快速传输协议]，在无线网络或网络环境较差的情况下可以使用，有一定的加速效果。

界面如下所示：

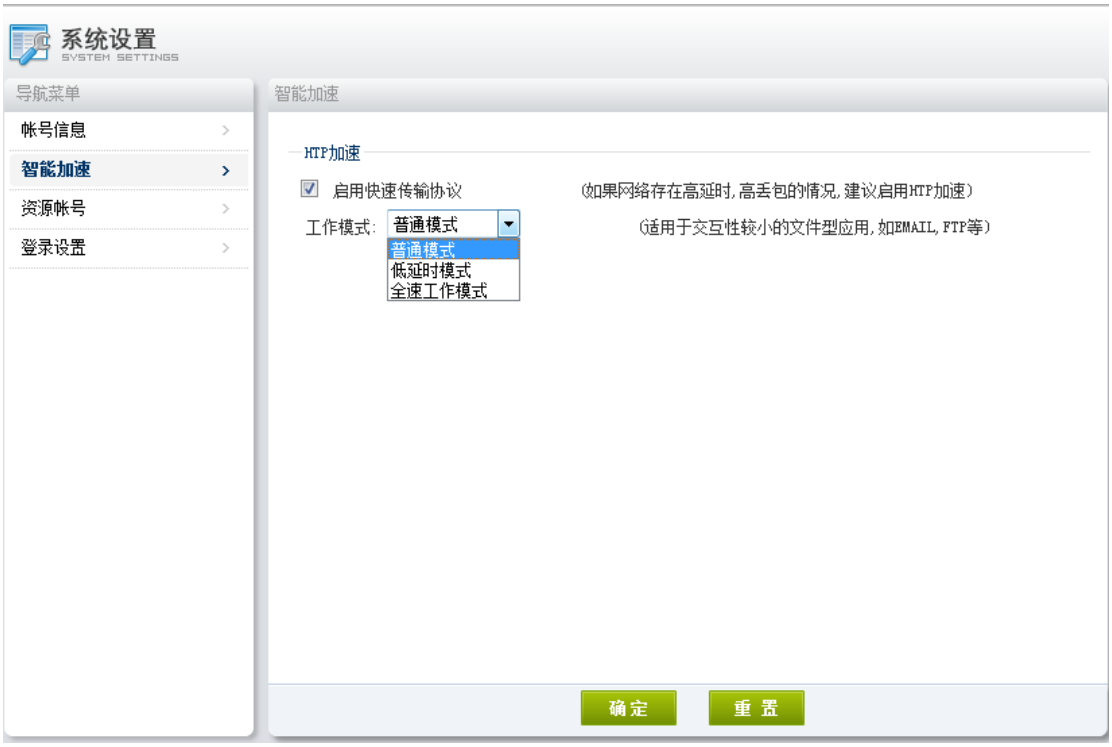
点击高级设置按钮，可定义启用快速速传输协议的参数。界面如下所示：

在『启用模式』中，勾选[自动选择]，并设置相应的丢包率和延时，则客户端接入 VDI

后会自动测试网络状况，判断是否需要启用快速传输协议传输。丢包率和延迟两个条件，只要符合其中一个条件则启用快速传输协议，一般保留默认值即可。

勾选『手动选择』后，需要在客户端手动开启该功能。

客户端接入 VDI 登录到服务页面，点击右上角的设置，选择[智能加速]，页面如下：



勾选[启用快速传输协议]按钮，并选择[工作模式]， 最后点击确定配置生效。

『启用快速传输协议』功能只有通过 IE 浏览器访问 VDI 才可以使用（不支持其他浏览器）；该功能需要通过 UDP 端口实现，在 VDC 设备单臂部署时注意在前置防火墙网关把此 UDP 端口映射到 VDC 设备上。

『单边加速设置』用来设置加速基于 TCP 隧道的服务。

勾选[启用单边加速]即开启单边加速功能。如下图：

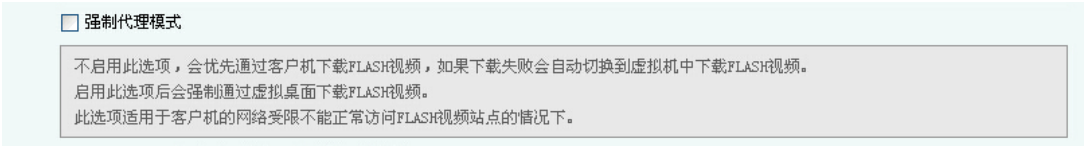
单边加速功能需要先在序列号中激活才可以选，否则会是灰色不可选状态。

3.5.3. Flash 重定向

『Flash 重定向』将 Flash 媒体将下载到 aDesk 客户机进行本地播放，从而提升 aDesk 带有 Flash 的网页的浏览效果。

『Flash 重定向』功能默认启用且对所有地址进行重定向。勾选“启用 Flash 重定向功能”可以启用或禁用该功能。

『强制代理模式』不启用此选项，会优先通过客户机下载 FLASH 视频，如果下载失败会自动切换到虚拟机中下载 FLASH 视频。启用此选项后会强制通过虚拟桌面下载 FLASH 视频。此选项使用于客户机的网络受限不能正常访问 FLASH 视频站点的情况下。



重定向范围可以选择“仅以下地址”（白名单方式）或“排除以下地址”（黑名单方式），地址填写支持以*和?进行通配，最多支持 128 条地址规则。

3.6. 时间计划

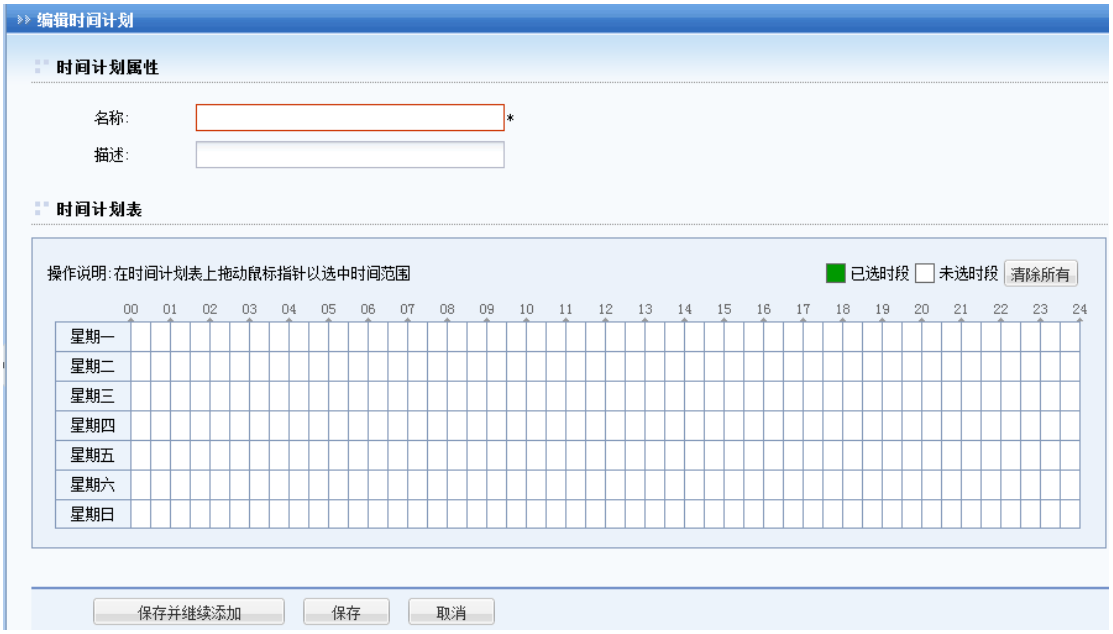
『时间计划』用于定义常用的时间段组合，这些时间组合可在『防火墙过滤规则设置』、『用户权限设置』和『端点安全规则』中使用，以设置相应的规则生/失效时间，该时间以设备当前时间为准。

WEBUI 路径：『系统设置』→『时间计划』。

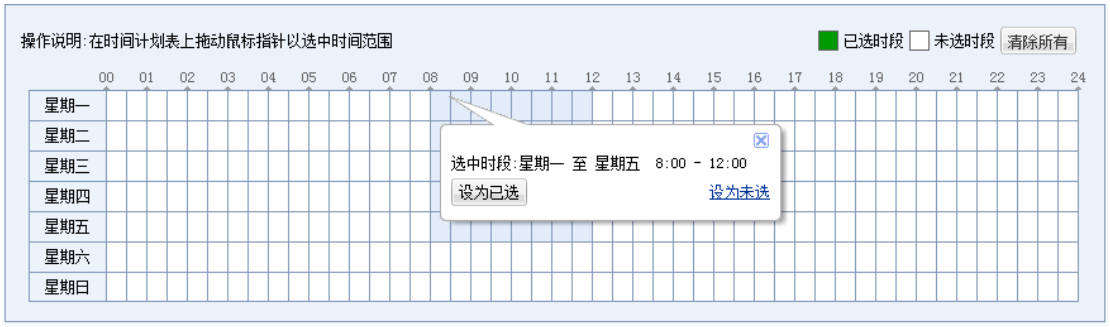
界面如下图所示：

例如需要定义：每周一至周五 8:00-12:00，14:00-18:00 为上班时间，配置方法如下：

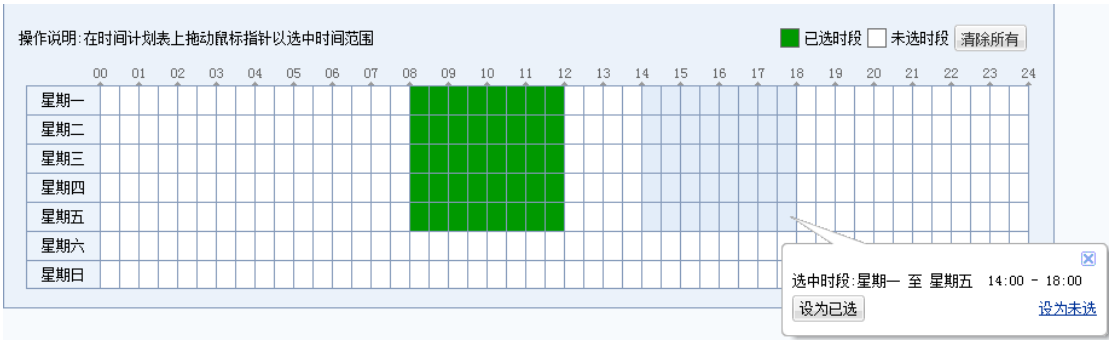
首先在时间计划里面点击新建，如下图所示：



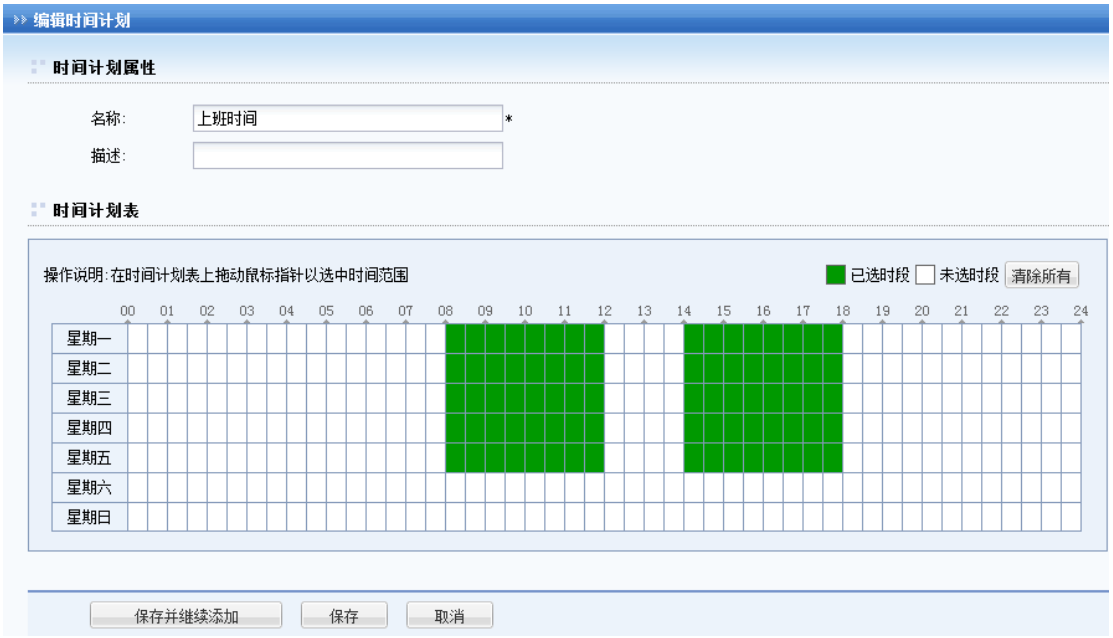
设置名称为“上班时间”，在时间计划表里面选择相应的时间小格，本例中先选中周一至周五 8:00-12:00 的小格，选择时间小格后会弹出选中时段的提示框，选择设为已选，如下图所示：



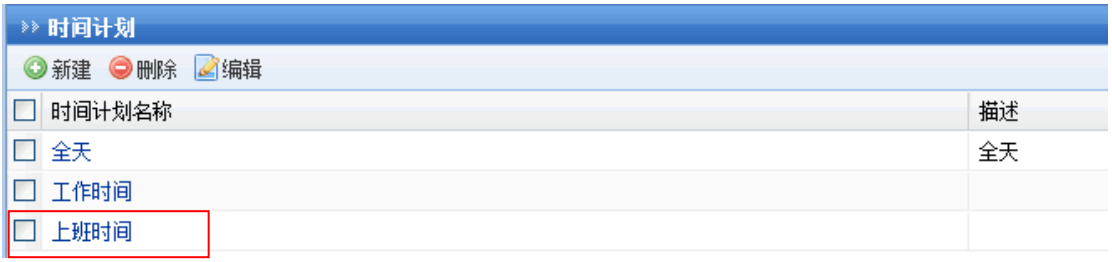
然后用同样的方法选择周一至周五 14：00-18：00 时间段，如下图：



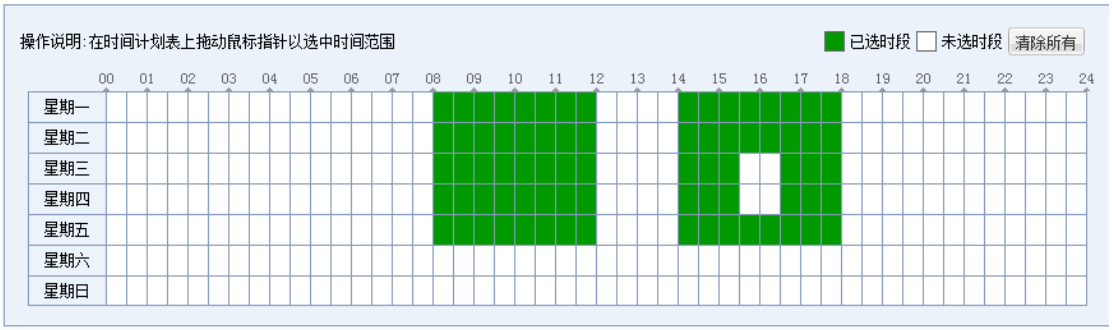
都设置完以后，即完成该例中“上班时间”的定义。



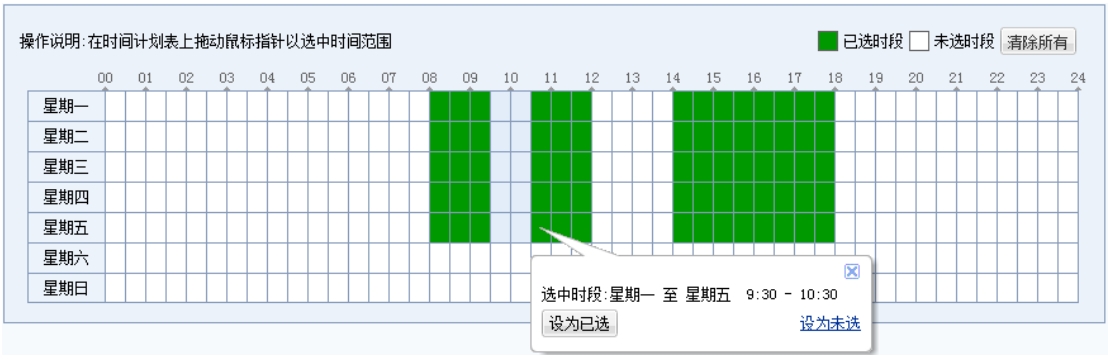
点击保存即可。设置完成后显示如下：



如果在时间计划中，需要删除某一个时间小格，直接点击该绿色小格，变成白色即可。绿色表示“已选时段”，白色表示“未选时段”。如下图所示：



如需在时间计划中删除某一段时间，则勾选该段时间小格，点击设为未选即可，如下图所示：



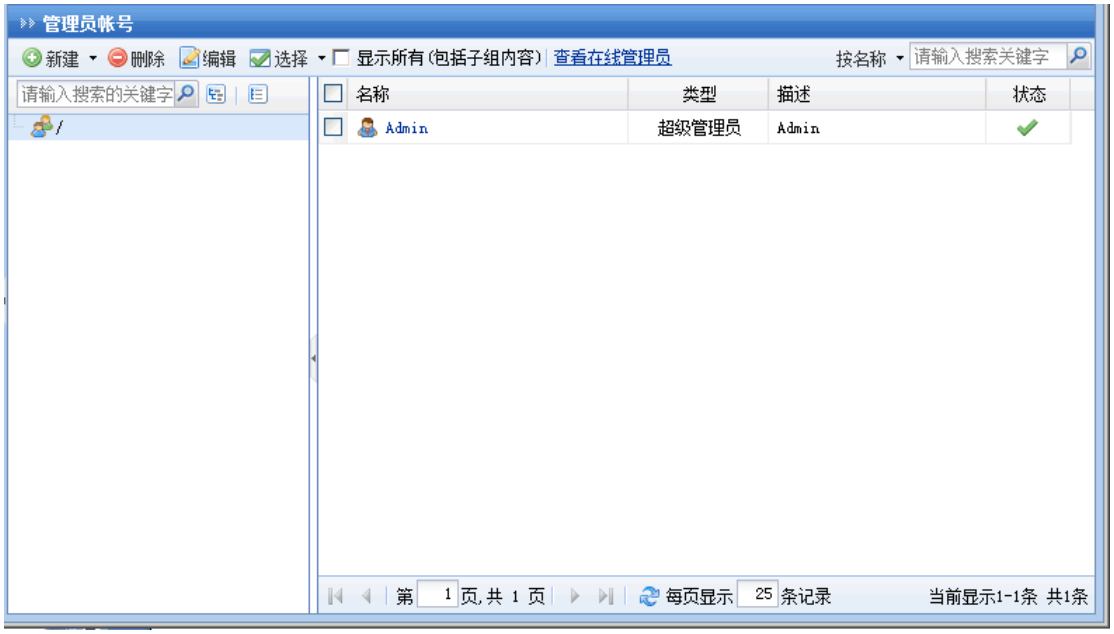
此处只是定义一个时间计划，然后再在 『VPN 有效时间』、『防火墙过滤规则设置』、『用户权限设置』、『端点安全规则』等设置中来引用该时间计划，引用的时候，只需要选择相应的时间计划名称即可。

3.7. 管理员账号

『管理员账号』用来设置登陆设备的管理员账号和密码等信息，可以把管理员归纳成管理组，并对管理员和管理组分配不同的权限。

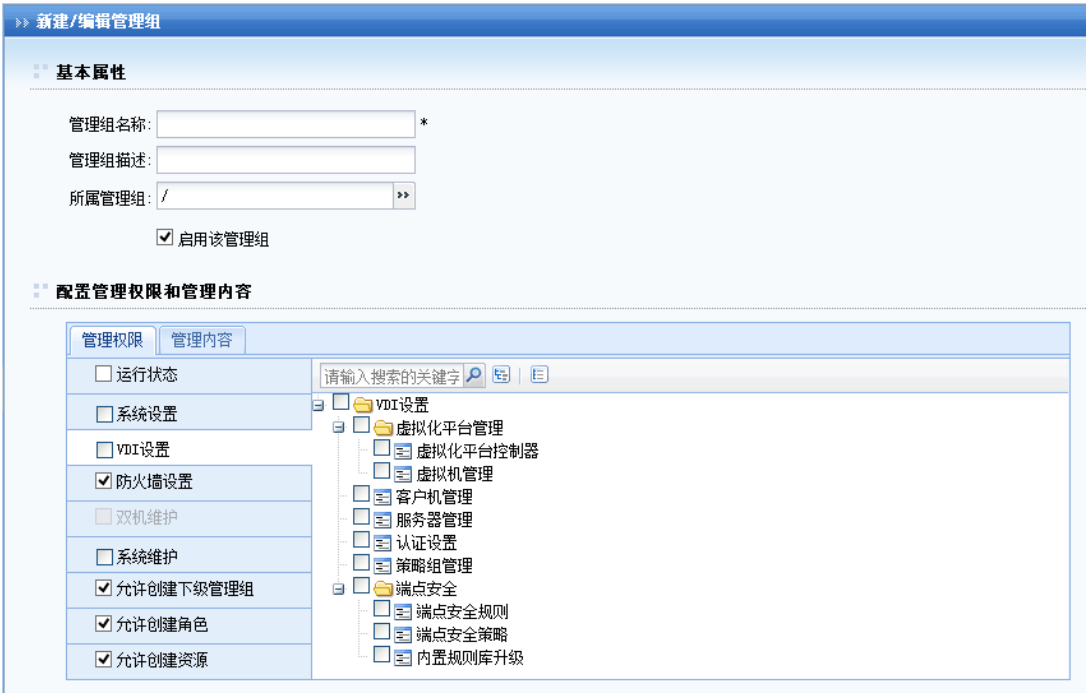
勾选[显示所有（包括子组内容）]即可显示出左边目录树所选中的组及该组下的子组的管理组和管理员信息。

选中管理员或者管理组，点击编辑，即可对该管理员或管理组进行编辑。点击删除，即可把选中的管理员或者管理组删除。显示如下：



点击新建后会出现[管理员]和[管理组]的选项，显示如下：

选择[管理组]后，可新建一个管理组并设置该管理组的权限。显示如下：

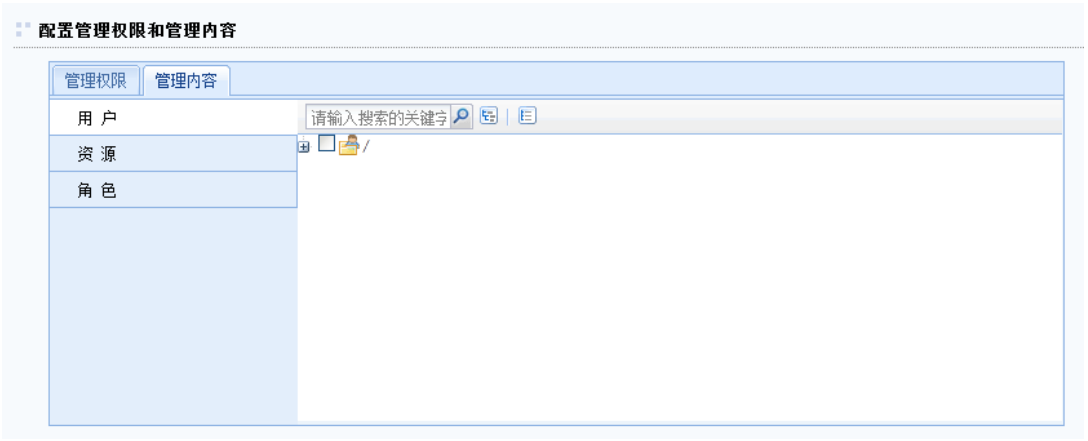


『管理组名称』和『管理组描述』可自定义。

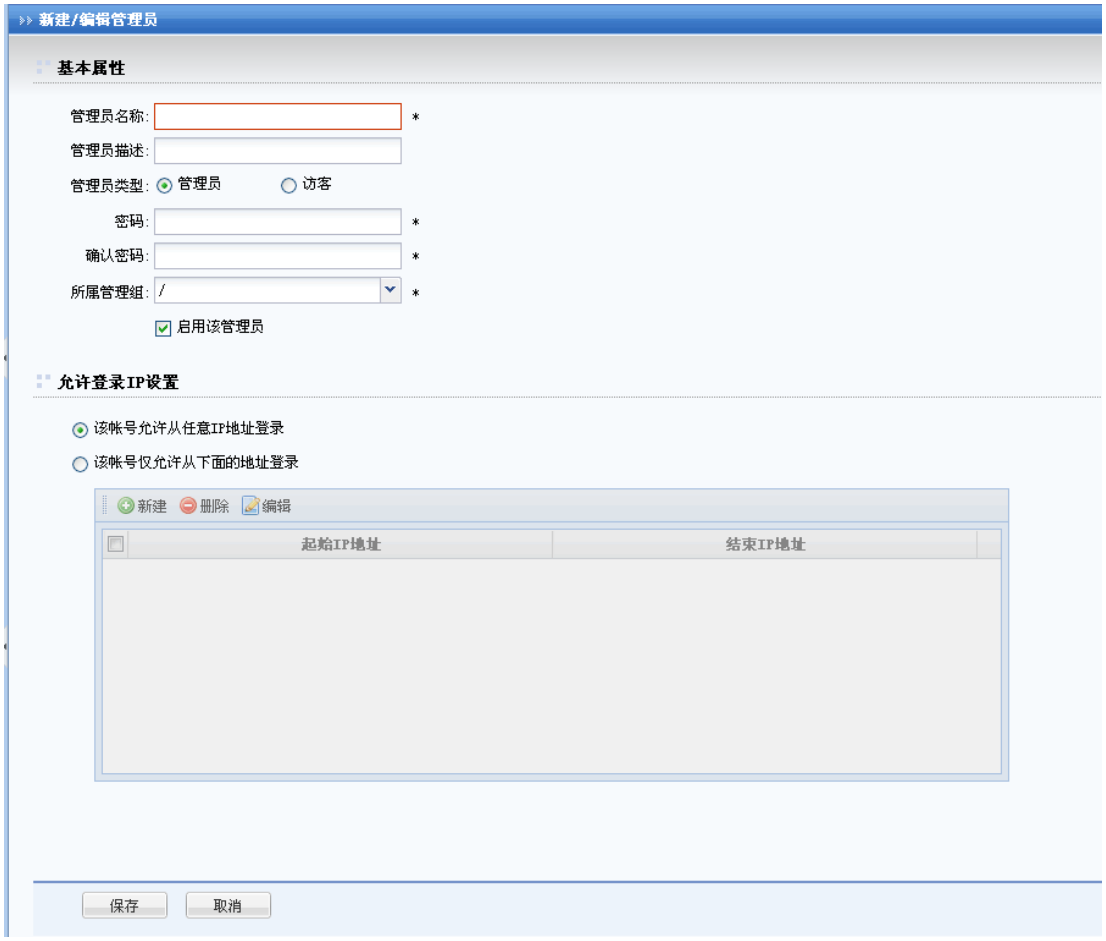
『所属管理组』：选择该管理组所属的组，若是在根组下建管理组，则保持默认即可。

【管理权限】里面可以设置该组成员能够管理设备的权限，只需在相应模块后打勾即可。

选择【管理内容】，即可对该组管理员管理的内容进行限制。包括用户，资源和角色的管理。显示如下：



点击新建管理员，出现如下设置页面：



『管理员名称』即管理员登录 VDC 设备控制台时所使用的帐号。

『管理员描述』设置该管理员的相关说明信息，可任意填写。

『管理员类型』分为[管理员]和[访客]，管理员对设备配置具有相应组的管理权限；访客只具备只读权限，只能看相应组权限下的设置信息。

『密码』和『确认密码』用于设定管理员登录的密码。

『所属管理组』设置此管理员所属的管理组，选择后可匹配相应组的权限。

『允许登录 IP 限制』可以设置使用此管理员帐号登录 VDC 设备的 IP 地址。若设置了登陆 IP 限制，那么在 IP 列表外的地址将不能使用该账号登陆 VDC 设备。

 **注意：下级管理组的管理权限不会比上级管理组还多。即下级管理组的可管理的用户、资源、角色均由上级管理组授权，不会超出这个范围。**

3.8. 集群部署

集群可以使一组相互独立的服务器在网络中表现为单一的系统，并以单一系统的模式加以管理。集群的各个节点（VDC 设备）由一个分发器和一组真实服务器组成，分发器和真实服务器都是 VDC 设备（分发器本身也是一台真实服务器）。网络客户接入 VDI 的时候，会由分发器合理的分配给集群中最空闲的真实服务器为客户提供服务。集群可以达到提高容量和性能的目的，为客户提供更高可靠性的服务。

3.8.1. 集群中的各元素定义与简介

集群：一组独立的计算机构成的一个松耦合的多处理器系统，通过协调通讯和数据同步实现分布式计算机。

分发器：集群中担任负载均衡器角色的设备。分发器同时也可以是一个真实服务器。

真实服务器：集群中担任真实服务器角色的设备。

节点：分发器和真实服务器的泛称。

集群 IP：集群的对外 IP 地址，外部用户通过这个 IP 来访问 VDC 设备。

集群密码：集群内部通讯密码，使用这个密码对集群内部的通信信息进行加密。

权值：节点性能指标，为 0 时表示不接收服务。

动态加权最小连接调度：各个服务器用相应的权值表示其处理性能。各节点动态地上报自身的权值。加权最小连接调度在调度新连接时尽可能使服务器的已建立连接数和其权值成比例。

3.8.2. 集群的主要特性

高性能：

1、 新连接会根据“动态加权最小连接”调度到服务节点。

2、 同一 IP 始终调度到同一节点，直到该 IP 与 VDI 断开，新连接才会重新调度到其它节点。

3 、分发器接收请求，然后把请求调度到真实服务器，真实服务器回应用户的请求。

高可用：

1 、节点故障后在心跳（LAN 口发出的信号）超时会被分发器从分发表中清除，只有在该机器接受服务的用户受影响。

2 、新节点加入集群后分发器会把它加入分发表。

3 、分发器故障后会由优先级（优先级一样看性能）最高的机器升级为分发器，只有在分发器接受服务的用户受影响。

服务一致性：

1 、新的节点加入集群会从分发器下载所有配置和数据，与分发器的数据保持一致。

2 、管理员只能登录分发器的控制台进行修改，即使管理员登录到服务节点对 VDI 也只有查看权限（除了集群的基本配置的页面配置）。

3、 用户对用户数据（用户密码、HARD ID、手机号）的修改会同步到所有节点。

4 、任何节点数据库的改动都会激发数据校验，校验以分发器为准，如果不同则重新从分发器下载配置和数据库，然后重新启动相关服务。

5 、以下配置和数据不会在集群间同步，只在集群中每个节点单独操作有效：快速配置、网卡设置、日志查看（可以使用日志中心）、序列号、网关运行情况（在节点信息页

面中显示）、重启网关（在节点信息页面中有对每个节点的重启）、保存配置和恢复配置、DHCP 状态。

6、没有数据库改动的操作不会进行数据校验，任何节点数据库的改动将会引起所有节点进行数据校验。

7、 时间同步，所有节点的实际以分发器的为准。

信息监控：

1 、分发器上能查看各个节点的资源使用情况，可以控制节点重启 VDI 或重启服务或重启机器。

2 、分发器上能查看在线用户列表及其所在节点，并有断开某个用户功能。

分发器热插拔：

1 、单个节点：单个节点会在两个心跳间隔内成为分发器。

2 、分发器热插拔：如果分发器故障，那么在两个心跳间隔内拥有最大权值的节点将成为分发器。

3 、分发器的抢夺机制：如果新加入节点被配置成为优先成为分发器，而且是集群内唯一被具有该优先级，那么该节点先成为真实服务器，然后在两个心跳间隔内成为分发器，原来的分发器则降级为真实服务器。

节点热插拔：

1、 节点接入集群：在一个心跳间隔内从分发器下载数据，解压，覆盖原来的数据，重启服务，进行数据校验，通过后校验后正式成为服务器。

2 、节点故障：在两个心跳间隔内，该节点会被分发器从分发表中剔除。

可靠性：

集群中只要有一台 VDC 网关正常运行，用户即可使用 VDI 的所有服务。使用固定集群 IP 时当某台主机故障后，其该节点上的在线用户会断线，需要重新登录。

3.8.3. 部署方式

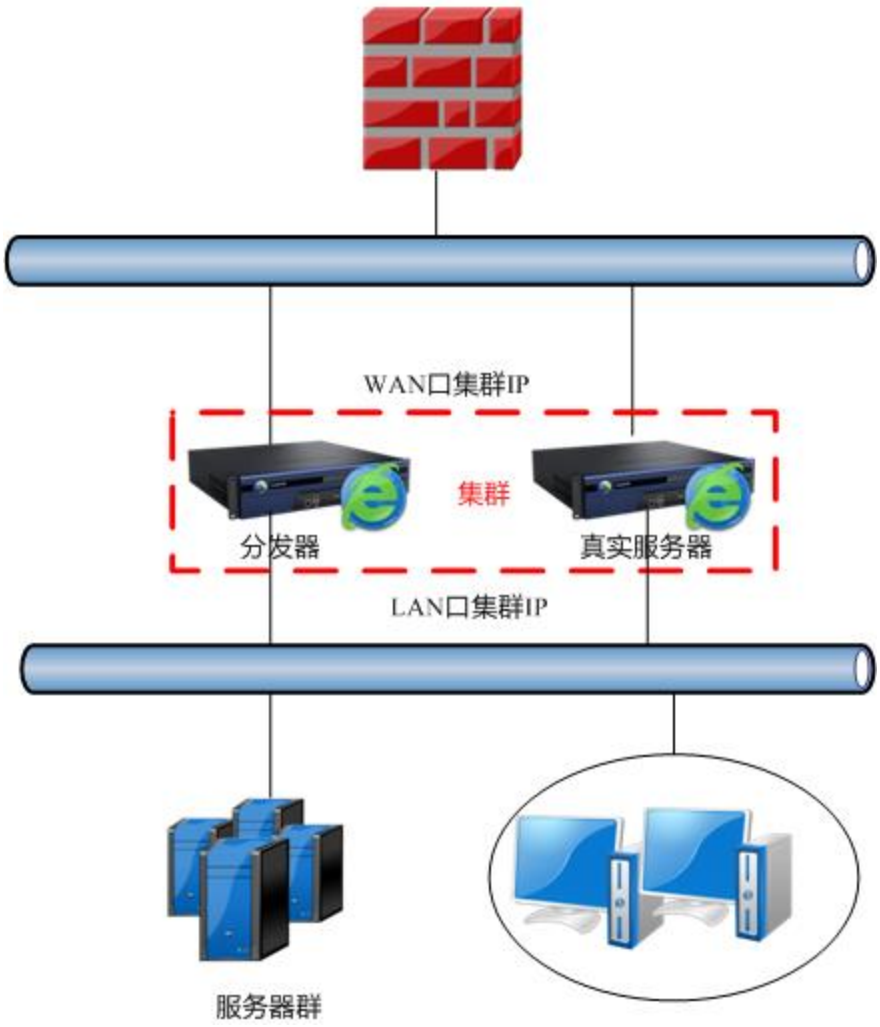
单臂模式部署：集群中各个 VDC 设备的内外网口设置参考章节 3.2.1 部署模式，其他其他部署与独立设备单臂部署相同。另外还需要在各个 VDC 设备的『集群部署设置』中的『基本配置』里配置相同的 LAN 口集群 IP。

单臂模式

注意：单臂模式部署时，集群中的所有 VDC 设备『内网接口配置』中设置的 LAN 口 IP 和『集群部署设置』里『基本配置』设置的 LAN 口集群 IP 必须在同一个网段。

网关模式部署：集群中各个 VDC 设备的内外网口设置参考章节 3.2.1 部署模式，其他其他部署与独立设备网关部署相同。另外还需要在各个 VDC 设备的『集群部署设置』中

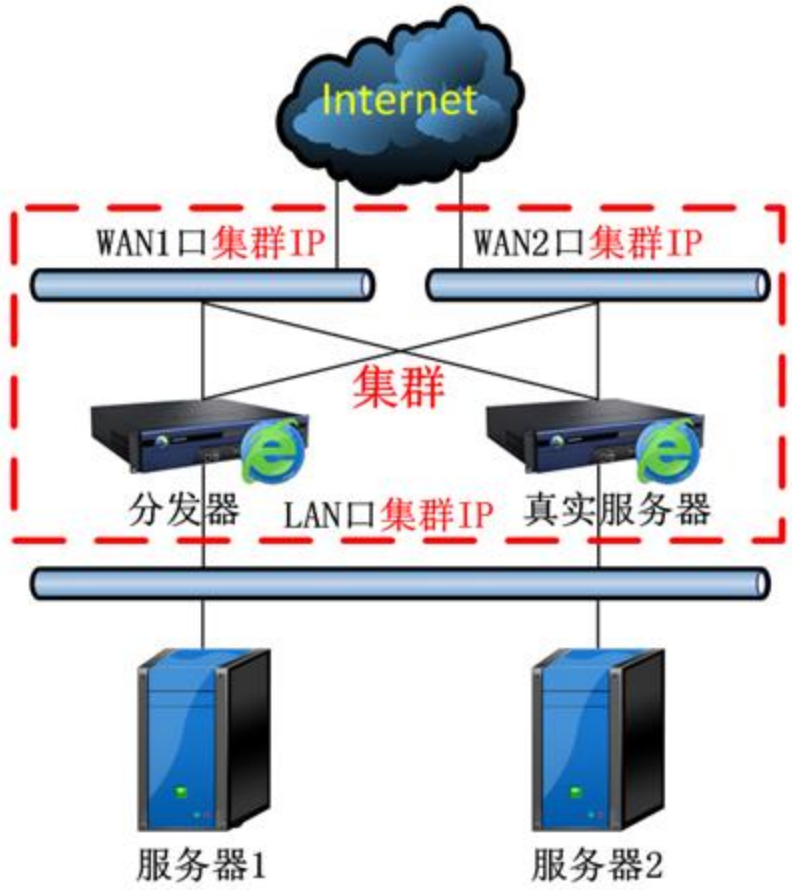
的『基本配置』里配置相同的 LAN 口集群 IP 和 WAN 口集群 IP。



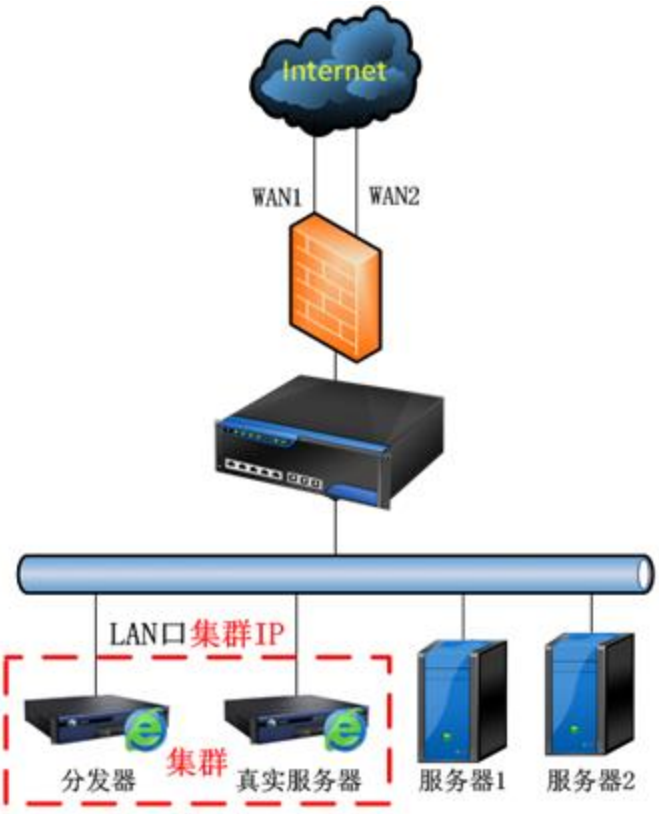
网关模式

注意：网关模式部署时，集群中的所有 VDC 设备『外网接口配置』中设置的 WAN 口 IP 需要在同一个网段，但是和『集群部署设置』中『基本配置』里设置的 WAN 口集群 IP 必须在不同网段。VDC 设备做网关时，若设备是拨号上网的情况，集群不支持。

多线路模式配置：集群中各个 VDC 设备的内外网口设置参考章节 3.2.1 部署模式，其，其他部署与独立设备多线路部署相同。需要在各个 VDC 设备的『集群部署设置』中的『基本配置』里配置相同的 LAN 口集群 IP 和 WAN 口集群 IP（有几个 WAN 口就填几个 WAN 口集群 IP）。


Internet
WAN1口集群IP
WAN2口集群IP
集群
分发器
LAN口集群IP
真实服务器
服务器1
服务器2

网关模式多线路



单臂模式多线路

注意：集群中每个节点填写集群 IP 时必须保持一致。

3.8.4. 集群部署设置

WEBUI 路径：『系统设置』→『集群部署』→『集群部署设置』。

首先需要在『集群部署』下的『集群部署设置』中进行相应的配置，每台需要加入集群的设备都需要进行这样的配置。操作界面如下：

『集群部署设置』中的『启用集群部署功能』可以开启或关闭 VDC 设备的集群功能。

『集群部署密钥』处填写该集群的密钥，每台需要加入集群系统的设备必须填写一致。集群密钥以作为分发器的 VDC 设备上设置的集群部署密钥为准。

『分发器选举规则』中可以设置[通过优先级选举分发器]和[优先做为分发器]。

若选[通过优先级选举分发器]，在[优先级别]的下拉框中可选择[自定义]，[高]，[中]，[低]，若选择自定义，则可以在后面填写优先级数字，数字越小，级别越高。集群中所有设备中，优先级越高的设备，则越优先被选为做分发器。

若选择[优先做为分发器]，则该台设备做为分发器，在同一个集群部署环境中，只允许一台设备选择该选项。

『集群 IP 设置』中可以设置各个网口的集群 IP，每一台加入到集群中的 VDC 设备，都必须填写相同的集群 IP。

『LAN 口集群 IP』中设置对外发布的 LAN 口的集群 IP。

『DMZ 口集群 IP』中设置对外发布的 DMZ 口的集群 IP。

『WAN1 口集群 IP』中设置对外发布的 WAN1 口的集群 IP，『WAN1 口掩码』中设置相应的 WAN1 口掩码信息。

『WAN1 口网关』中设置相应的 WAN1 口的网关信息。

注意：集群 IP 是一组 VDC 设备组成的集群系统对外发布的 IP，集群中的每台设备在『集群 IP 设置』的设置都必须保持一致。

点保存使配置生效。

3.8.5. 集群部署状态

WEBUI 路径：『系统设置』→『集群部署』→『集群部署状态』。

『集群部署状态』中会显示集群中分发器和真实服务器的各种实时状态信息，包括节点 IP，节点类型，VDI 运行状态，各个节点的 CPU 使用率，各个节点的授权数，各个节点的在线人数，总在线人数，总授权数。操作界面如下：

点击登陆此节点打开这个节点控制台界面。

3.8.6. 集群在线用户

WEBUI 路径：『系统设置』→『集群部署』→『集群在线用户』。

『集群在线用户』中可以查看接入 VDI 的用户名称、接入 IP、接入节点、接入时间，并可以对接入的用户进行断开连接操作。操作界面如下：

『节点选择』可以选择要查询的节点，默认为所有节点。

立即刷新刷新当前在线用户信息。

断开连接可以对该用户进行断开 VDI 连接的操作。

锁定用户数可以查看被锁定的用户数量。

查看锁定用户可以查看被锁定的用户。

页面右上方的放大镜框中可输入目标用户的关键字，点击放大镜图标，可进行搜索。

第4章 VDI 设置

『VDI 设置』包含『虚拟化平台管理』、『客户机管理』、『服务器管理』、『用户管理』、『资源管理』、『角色授权』、『认证设置』、『策略组管理』、『端点安全』等部分。

VDI 设置的核心内容是三部分，分别是『用户管理』、『资源管理』和『角色授权』。三者间的关系是：通过“角色”把“用户组”（或“用户”）和“资源”关联起来，“用户组”内的“用户”获得相应“资源”的访问权限。

4.1. 虚拟化平台管理

『虚拟化平台管理』包括虚拟化平台控制器管理和虚拟机管理。

4.1.1. 虚拟化平台控制器

WEBUI 路径：『VDI 设置』→『虚拟化平台管理』→『虚拟化平台控制器』。

点击新建，弹出【新建虚拟化平台控制器】页面，如下图：

『名称』定义该虚拟化平台控制器的名称。

『描述』虚拟化平台控制器的描述，方便记忆。

『控制器地址』虚拟化平台控制器的 IP 地址，该地址须与虚拟桌面接入管理系统能正常通讯。

『连接帐号』虚拟化平台控制器的管理员用户名称，用于登录控制器时做身份验证。

『密码』虚拟化平台控制器的管理员密码，用于登录控制器器时做身份验证。

配置完成，点击测试连接可以测试虚拟化平台控制器是否连通，正常后点击保存，保存配置，或者保存并继续添加以保存当前配置并打开新的新建页面。

点击保存，再点击配置生效，保存并生效设置，虚拟化平台控制器建立完成。

勾选需要删除的虚拟化平台控制器，然后点击删除可以将不需要的控制器进行删除操作。

勾选需要编辑的虚拟化平台控制器，然后点击编辑，或者直接点击需要编辑的虚拟化平台控制器的名称，可以打开编辑页面，对控制器信息进行修改。

点击控制器地址，可以打开虚拟化平台控制器的控制台页面。

4.1.2. 虚拟机管理

在【虚拟机管理】页面，可以查看已添加的虚拟化平台控制器管理范围内的所有虚拟机运行状态，包括虚拟机开关机状态、虚拟机名称、所属的虚拟化平台、所属的资源、IP 地址、CPU、内存和磁盘占用，以及关联的用户等信息，在虚拟机管理列表界面可以查看独享桌面资源列表和对应资源派生的虚拟机，如下图：

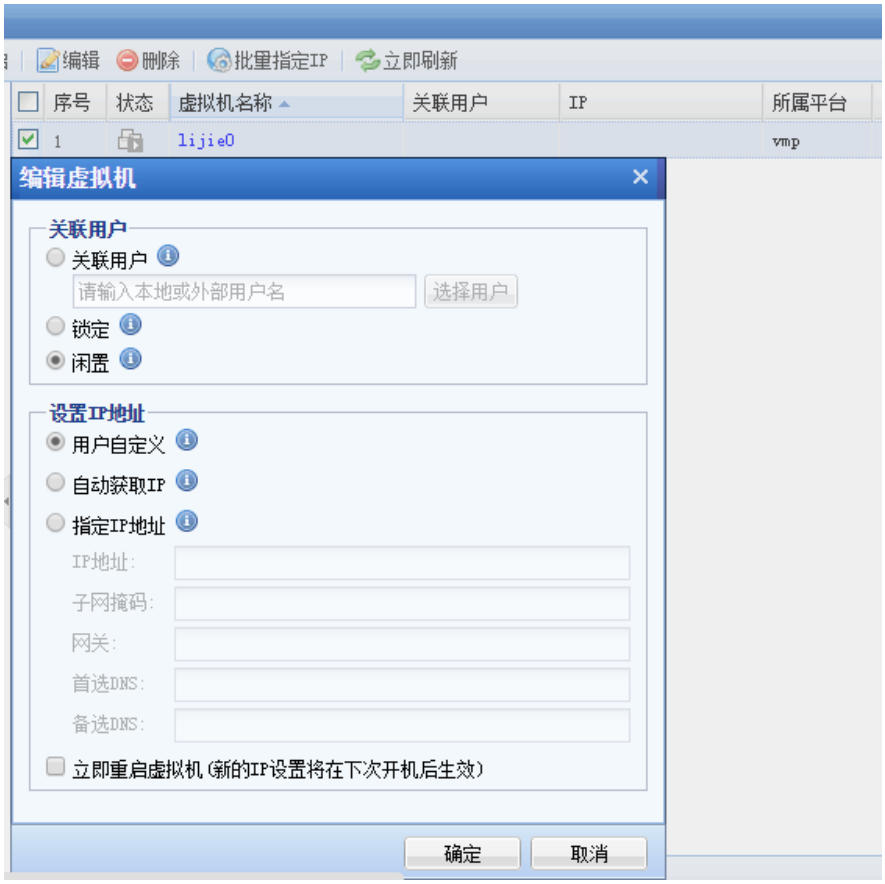
开机 将所选择的虚拟机进行开机操作。

挂起 将所选择的虚拟机进行暂停操作，暂停后虚拟机当前状态会保留，但不能被访问，也不占用虚拟机控制器的资源。

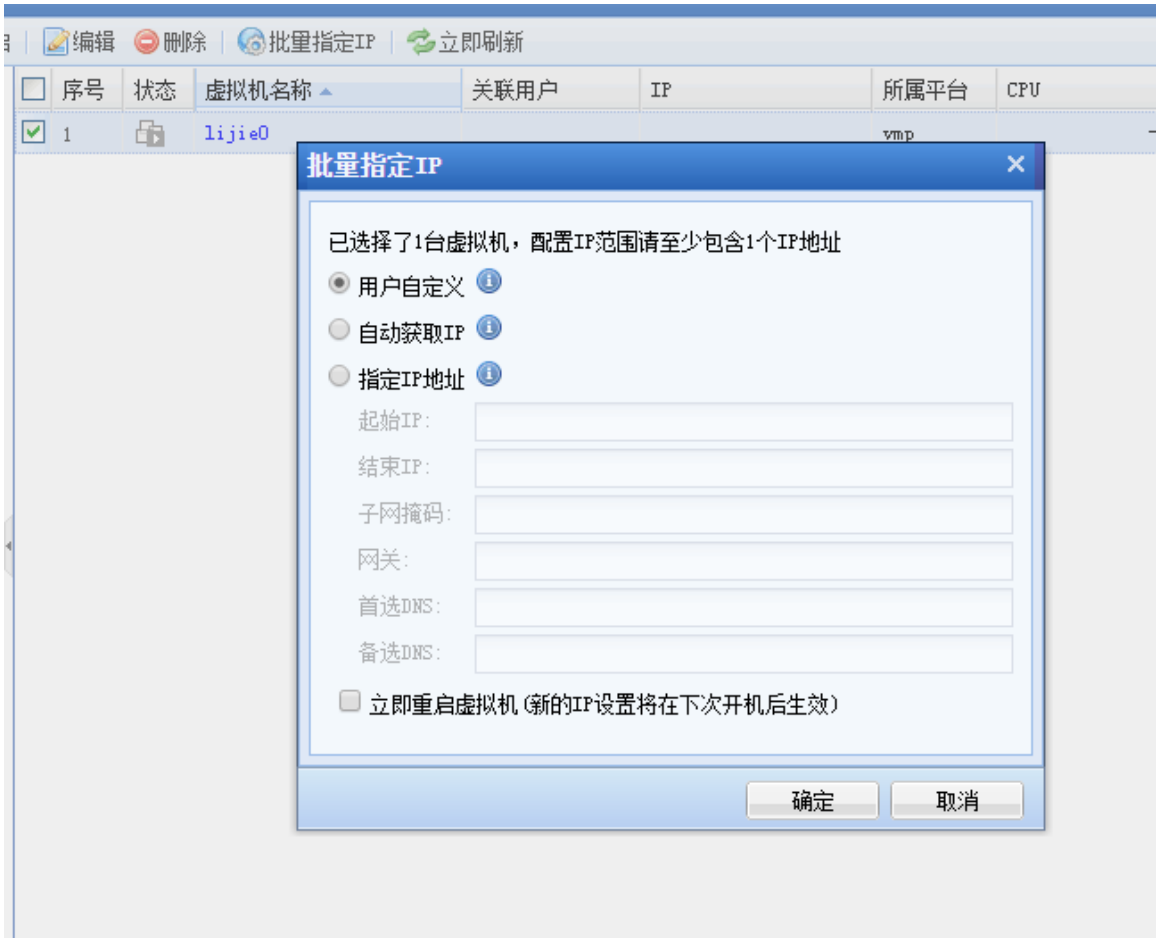
关机 将所选择的虚拟机进行关机操作。

重启 将所选择的虚拟机进行重启操作。

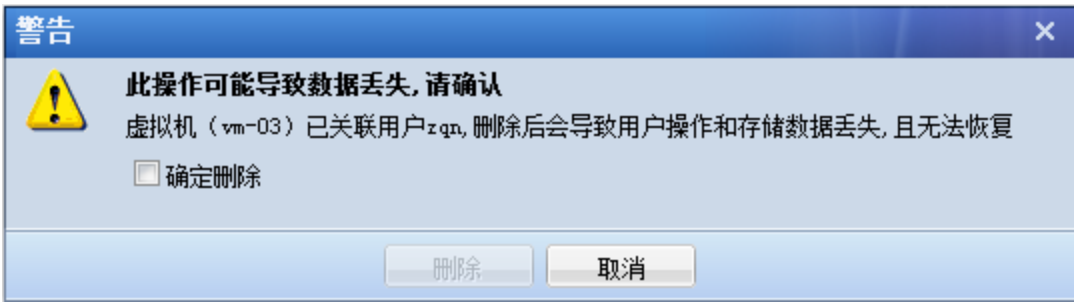
编辑 对单台虚拟机进行编辑，主要满足客户对单台虚拟机制定关联用户的需求，其次还可以对虚拟机进行锁定闲置操作，满足客户对单台指定 IP 功能，设置自动获取 IP 地址和用户自定义 IP 设置。如下图：



批量指定IP 对多台虚拟机进行批量制定 IP 操作，满足客户对多台虚拟机进行指定 IP 段，设置自动获取 IP 地址和自定义 IP 地址操作。如下图：



删除 将所选择的虚拟机进行删除操作。点击删除时，会弹出如下警告，需勾选确认删除后，才能继续点击删除完成操作。



立即刷新 刷新当前显示的虚拟机的运行状态等信息。

右侧下拉列表中可以选择虚拟机状态，根据状态进行过滤显示。或者在输入框中输入关键字，根据关键字进行搜索过滤。

4.2. 客户机管理

『客户机管理』用于配置管理接入 VDC 设备的 aDesk 瘦客户机。

WEBUI 路径：『系统菜单』→『VDI 设置』→『客户机管理』。页面如下：

在该页面可以查看接入 VDC 设备的 aDesk 瘦客户机的序列号、描述、IP 地址、MAC 地址、最近登录帐号、接入断开时间，以及在线状态等信息。左侧有瘦客户机分组，支持新建，编辑和删除组。

点击删除，用于删除已接入的客户机。

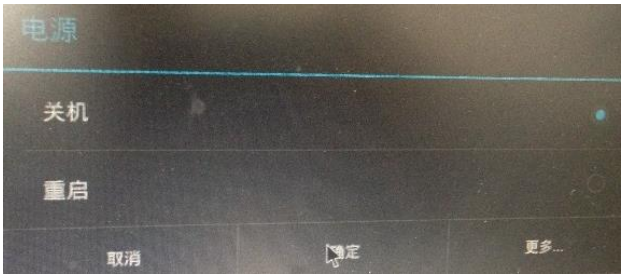
点击编辑，用于编辑所勾选的客户机的描述信息等。

点击移动，移动瘦客户机。

点击关机，可以让瘦客户机批量关机，关闭瘦客户机的时候同时关闭用户当前虚拟机。

点击获取日志，用于从所勾选的客户机获取运行日志等，通常用于故障排查。

瘦客户机导航栏具有重启按钮，当虚拟机系统未响应，卡死等异常时，可以点击该按钮重启虚拟机尝试恢复。



瘦客户机有关机重启和更多选项，可以在设置隐藏导航条时用户可以通过瘦客户机电源键操作进行关闭/重启虚拟机，瘦客户机。

4.3. 服务器管理

『服务器管理』用于配置 [资源服务器]和[存储服务器]。添加终端服务器前，需先在服务器上安装“终端服务”组件和“RemoteAppAgent”程序，并保证该程序能正常运行。

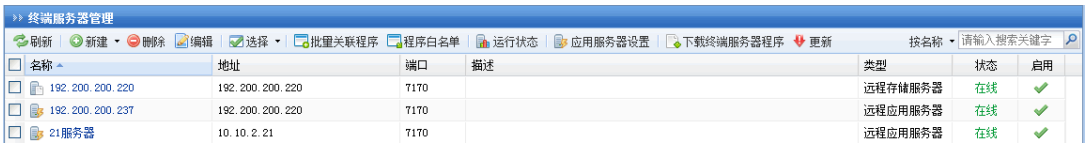
[资源服务器]在远程应用发布时，实现将服务器的应用程序作为资源发布给用户，用户接入后，即使客户端电脑上没有安装相应的应用程序也可以使用此应用。

[存储服务器]用来存储通过远程应用资源修改的文档，可创建[个人目录]和[公共目录]。

[个人目录]：每个用户每次登录都能看到属于自己的唯一私人存储目录，用户有对其完全控制的权限，可以在其下自己创建子目录，新增、删除文件或文件夹。

[公共目录]：所有用户均能看到与其关联的公共存储目录，读取其中的文件，管理员可以对用户是否有写权限进行控制，有写权限便可以保存文件到公共存储目录。

WEBUI 路径：『系统菜单』→『VDI 设置』→『服务器管理』。页面如下：



『名称』显示终端服务器的名称。

『地址』显示终端服务器的 IP 地址。

『端口』显示与终端服务器的通信端口。

『描述』显示对终端服务器的描述。

『状态』显示终端服务器的状态，包括[在线]或[脱机]。

『启用』显示终端服务器是否启用，包括[启用]或[禁用]。

点击删除，用于删除所勾选的资源服务器。

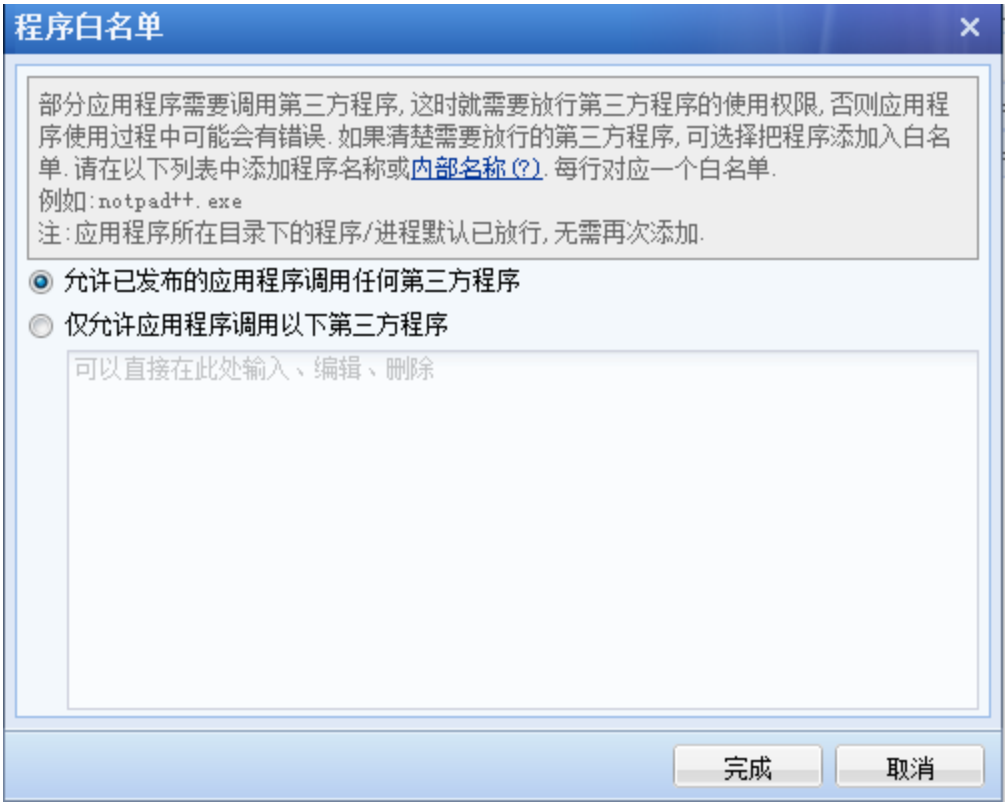
点击编辑，用于编辑所勾选的资源服务器。

点击选择，可选择所有页或选择当前页，也可取消选择，如下图：

点击批量关联程序，用于批量添资源服务器的应用程序，可以勾选多个资源服务器批量添加。

注：只有[在线]状态的资源服务器，才能设置批量关联程序。

点击程序白名单，用于设置所发布的程序允许调用哪些第三方的应用程序。如下图：

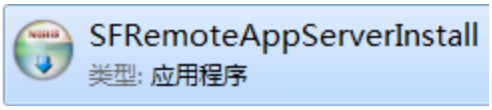


若选择[仅允许应用程序调用以下第三方程序]，则需要在下面的编辑框内输入相应的程序名称，格式请参考上面备注中的案例。

点击运行状态，用于查看资源服务器的运行状态，点击此按钮，直接跳转到『运行状态』→『VDI 运行状态』→『远程应用』页面。

点击应用服务器设置，用来设置是否启用应用服务器的会话保持和会话复用，并选择相应的负载均衡策略，如下图：

点击下载终端服务器程序，即可下载终端服务器安装程序下载到本地，如下图，双击可直接安装。

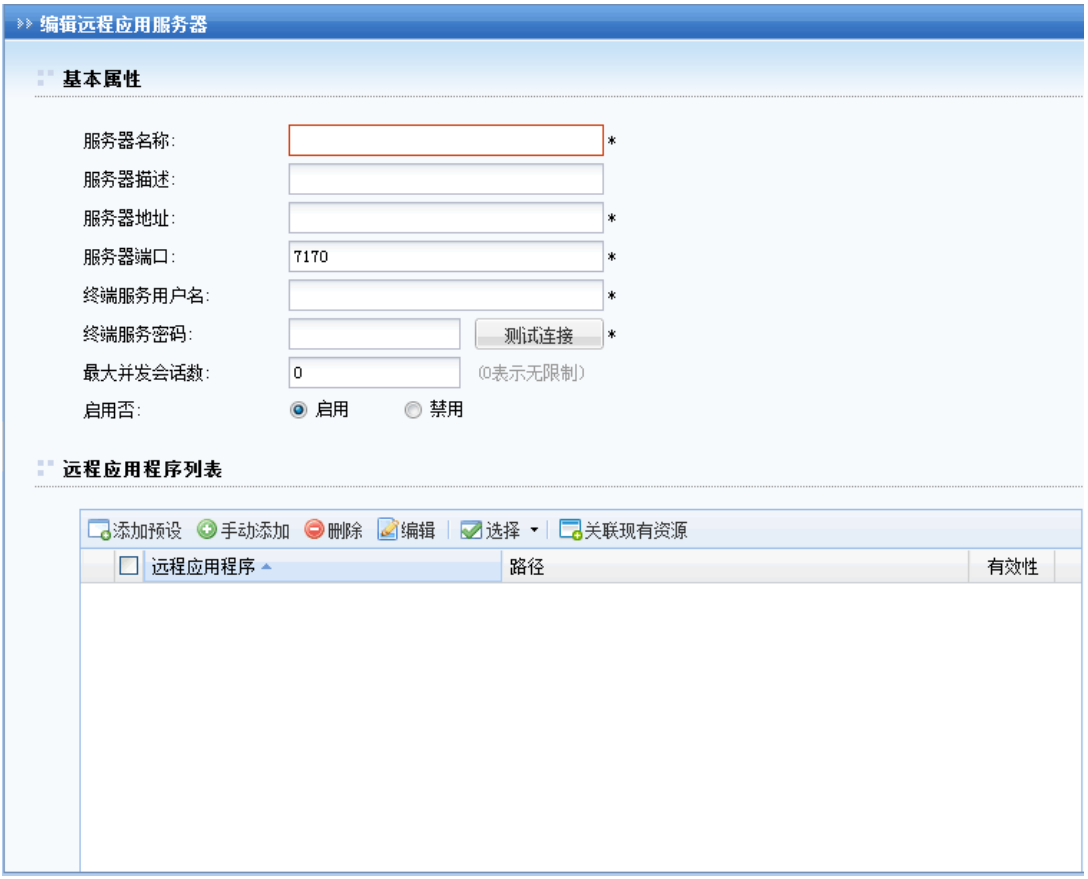


在终端服务器列表中的勾选某台服务器，点击更新，可以在 VDI 控制台升级该终端服务器。

点击新建，可新增[资源服务器]和[存储服务器]。页面如下所示：

4.3.1. 新增资源服务器

点击新建，选择[资源服务器]，弹出【编辑资源服务器】页面，如下图：



『服务器名称』定义该资源服务器的名称。

『服务器描述』资源服务器的描述，方便记忆。

『服务器地址』资源服务器的 IP 地址，该地址须与 VDI 能正常通讯。

『服务器端口』资源服务器的通信端口，用于 VDI 与服务器进行通信。默认端口为 7170，可以手动更改。

『终端服务用户名』远程终端服务器的管理员用户名称，用于登录服务器时做身份验证。

『终端服务密码』远程终端服务器的管理员密码，用于登录服务器时做身份验证。

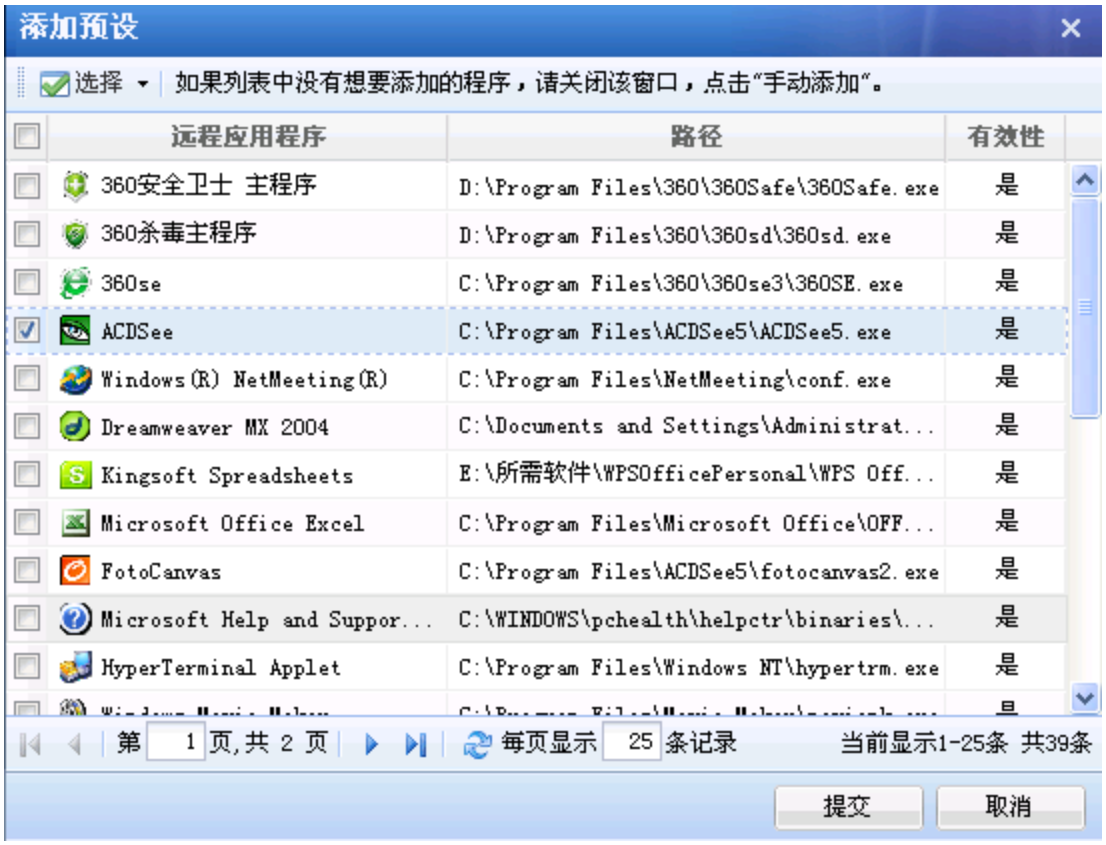
『最大并发数』远程终端服务器的用户同时访问的数量。

『启用否』选择是否启用该终端服务器，选择[启用]或[禁用]。

『应用程序列表』用于添加终端服务器发布的应用程序。

点击添加预设，打开【添加预设】对话框，选择需要发布的应用程序。

页面如下所示：

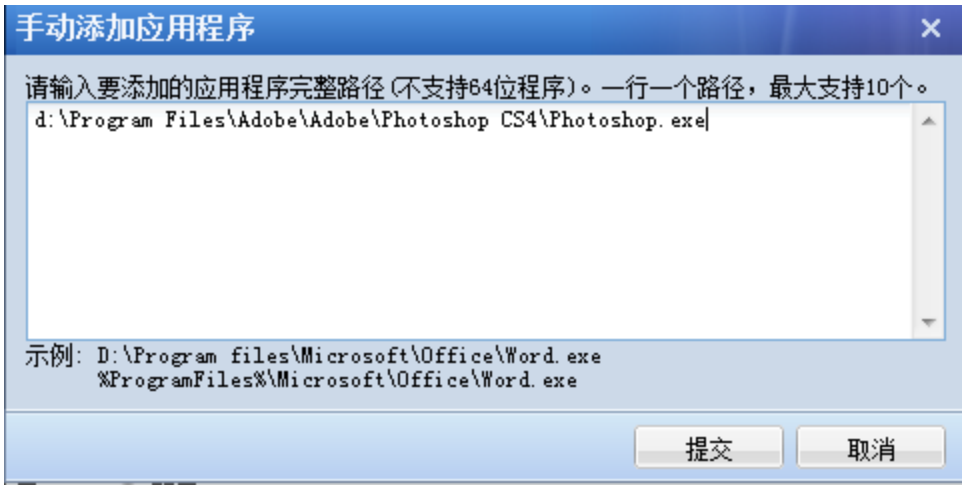


配置完成，点击提交，保存配置。

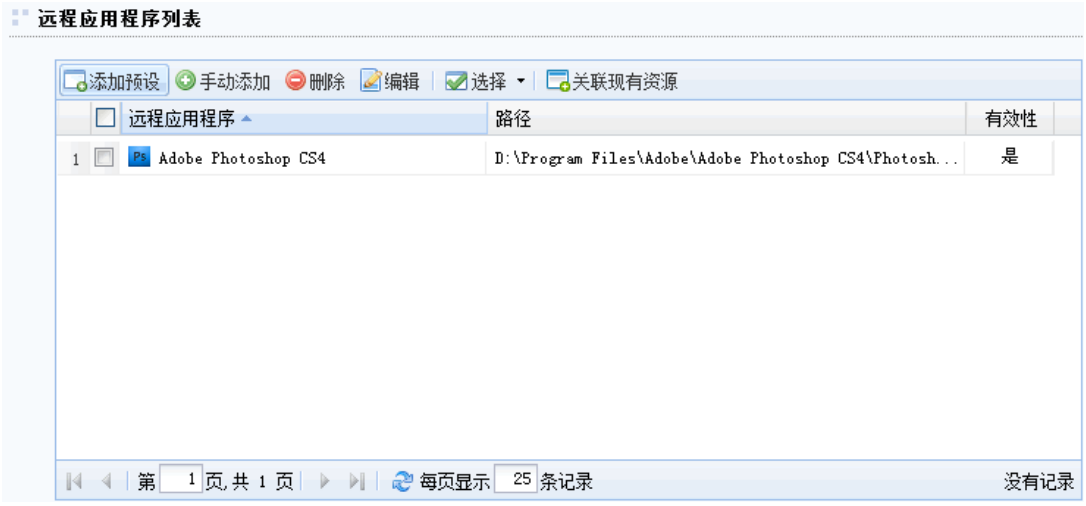
点击保存，再点击配置生效，保存并生效设置，资源服务器建立完成。

点击手动添加，可以手动添加应用程序完整路径。

页面如下所示：



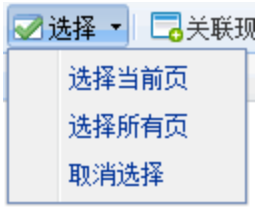
点击提交，将应用程序添加到应用程序列表。页面如下所示：



点击删除，用于删除所勾选的应用程序。

点击编辑，用于编辑所勾选的应用程序。

点击选择，可选择当前面或所有页，也可用来消息选择，如下图：



关联现有资源，用于快速关联现有资源，点击后弹出【资源列表】对话框，该资源列表中列出与『远程应用程序列表』所选择的资源的应用名称相同的资源。

配置完成后，点击保存，再点击配置生效，保存并生效设置，完成资源服务器建立。

终端服务相关资源的发布，请参考 4.5 章节。

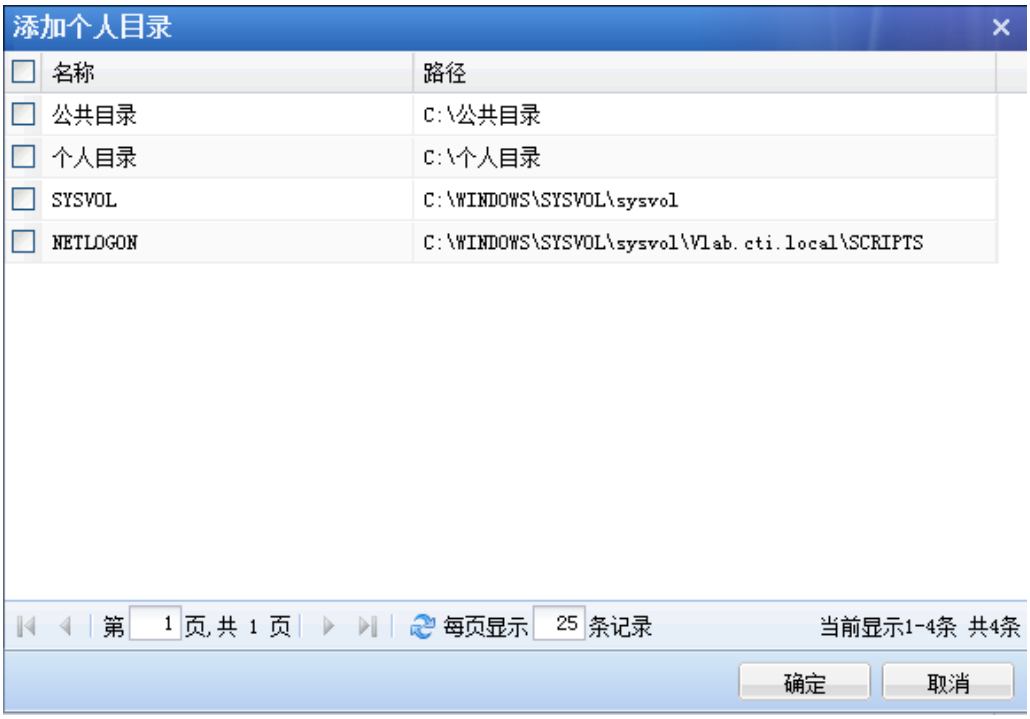
4.3.2. 新增存储服务器

在【服务器管理】页面，点击新增，选择[存储服务器]，弹出【编辑存储服务器】页面，如下图：

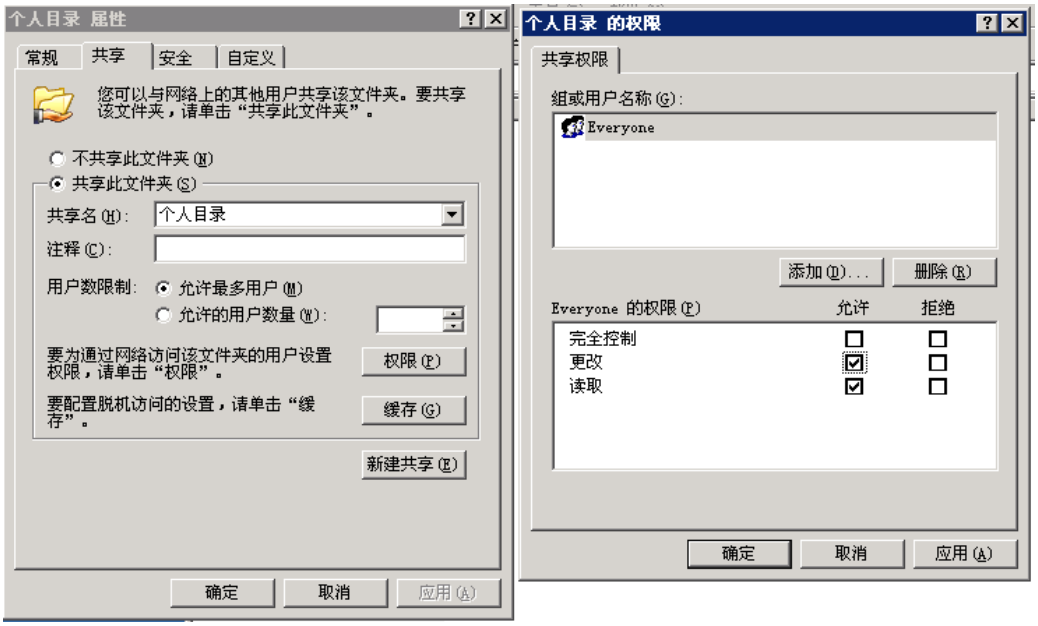
『基本属性』配置参考新增资源服务器，此处不再赘述。

『远程存储目录列表』，用于添加存储服务器目录，点击添加，可选择添加[个人目录]或[公共目录]，如下图：

选择添加[个人目录]，弹出【添加个人目录】编辑框，列出在终端服务器上可选择的目录：



注：该目录为终端服务器上设置为允许共享的目录，目录权限可以在终端服务器上设置，如下图：



用同样的方法，添加[公共目录]，添加好以后如下图：

最后，保存配置，并点击立即生效，使配置生效。即完成了存储服务器的添加。

存储服务器的使用，请参考 4.5 章节。

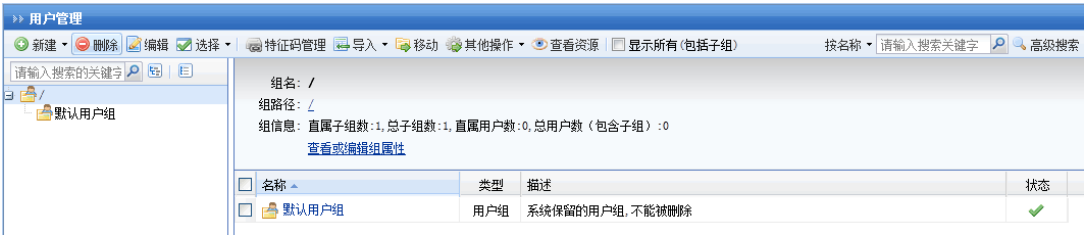
4.4. 用户管理

『用户管理』用于建立 VDI 用户和用户组，SANGFOR VDC 用“组策略”管理和设置

具有相同性质的用户。为了管理具有某些共性的用户以及更符合企业内部管理结构，采用分层的用户组管理用户。

WEBUI 路径：『控制台』→『VDI 设置』→『用户管理』。

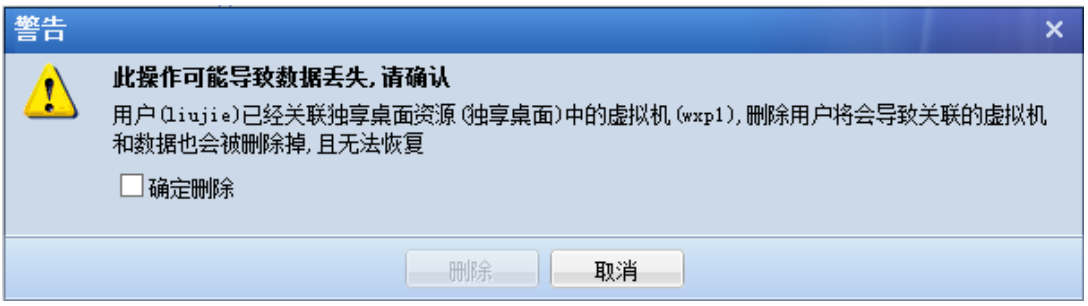
界面如下图所示：



在『用户管理』页面，左边为用户组结构树，右边为当前光标停留的用户组中的用户以及下级用户组。勾选[显示所有（包含子组）]，则显示当前用户组下的所有子组以及包含的所有用户。

用户组结构树上方的搜索框中可输入目标用户组的关键字，点击放大镜图标进行搜索，搜索到的用户组在用户结构树中会被高亮显示。

将所选择的用户进行删除操作。点击删除时，会弹出如下警告，需勾选确认删除后，才能继续点击删除完成操作。



4.4.1. 新建用户组

点击新建按钮，在下拉框中选择用户组，弹出【新增用户组】编辑框。

WEBUI 路径：『VDI 设置』→『用户管理』。

界面如下图所示：

『名称』即标识该 VDI 用户组的名字，必须填写。

『描述』可任意填写用户组的相关说明信息。

『所属组』在其下拉框中可选择当前新建用户组所隶属的用户组。/表示根组。

『最大并发用户数』控制该用户组及其下级组可以同时登录的在线用户数。

『账户状态』中勾选[启用]激活该用户组；勾选[禁用]禁用该用户组。

勾选[继承上级用户组关联角色、认证方式和策略组]，当前用户组自动关联上级用户组的角色、认证方法、策略组。

勾选[继承上级用户组认证方式]，当前用户组『认证选项』标签内的功能项与上级用户组一致。

勾选[继承上级用户组策略组』]，当前用户组『接入策略组』标签内的功能项与上级用户组一致。

勾选[继承上级用户组关联角色]，当前用户组自动关联上级用户组的角色。

『认证选项』标签内是用户组的登录认证方式的相关设置。

『多认证方式』分为[同时使用]和[任意一种]两种方式。

[同时使用]是“与”的关系，表示可以多种主要认证同时使用。

[任意一种]是“或”的关系，表示选择任意一种认证方式进行认证。

『主要认证』至少要选一种，『辅助认证』可选可不选。

[用户名/密码]认证，要求该用户组在建立用户账号时，设置用户账号的『名称』和『密码』。

[数字证书/Dkey 认证]，要求该组的用户账号都必须生成数字证书文件或生成USB-Key（有驱 USB-Key 或无驱 USB-Key）。

［外部认证]，在右边的下拉框中选择该用户账号所在的“外部认证服务器”。用户帐

号必须在所选择的认证服务器上存在。（需要先配置外部认证服务器，外部认证服务器的具体设置可参考 4.7“认证设置”章节）。

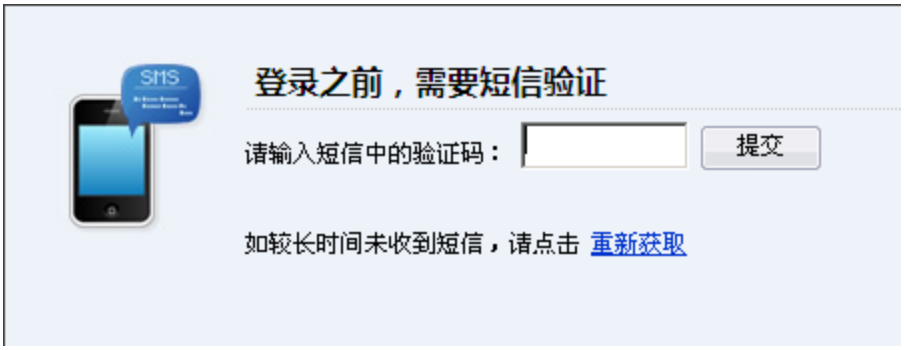
设置如下图所示：

1.认证服务器必须预先在『认证设置』界面设置完成 LDAP 或 Radius 认证服务器的相关参数。

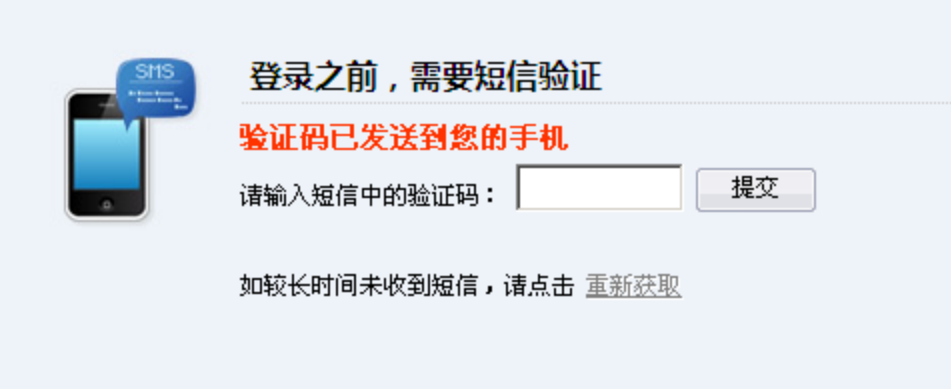
2. 『用户名/密码』认证和『外部认证』是互斥的关系，二者只能选其一。

[硬件特征码]把 VDI 用户账号和计算机的部分硬件特性（如网卡、硬盘等）生成的硬件特征码一一绑定。由于硬件特性的唯一性，使得该硬件特征码也是唯一的、不可伪造的。一个用户可以拥有多个特征码，即在同一个账号下，多台符合条件的电脑可以登录。也可以配置成只能拥有 1 个特征码。通过对该硬件特征码的验证，就保障了只有指定的硬件设备才能接入授权的网络，避免了安全隐患。

[短信认证]，要求该用户组在建立用户账号时，必须设置好用户账号的『手机号码』，（手机号码设置请参考 4.4.2）。当用户采用有效的认证方式登录 VDI 界面后，系统会以短信方式发送一个“校验码”到该用户的手机上，该用户必须输入正确的校验码完成登录。



若收不到短信，可以点击重新获取按钮，再次发送认证短信。



注意：认证设置中手机号码为空时将默认不启用短信认证，只有填上手机号码，且“认证方式”勾选短信认证，配置好短信认证模块，才真正启用。每一个用户账号只支持填一个手机号码。程序内部默认在手机号码前自动带上“86”（中国“国际区号”），若目标手机号为国外号码，必须填写相应国家的“国际区号”（短信认证模块的具体配置，请参照 4.7.2.1“短信认证配置”章节）。

[动态令牌]，出现以下配置界面，在下拉框选择该用户账号所在的“外部认证服务器”，服务器类型必须为“RADIUS 服务器”。用户帐号必须在所选择的认证服务器上存在。（外部认证服务器的具体设置可参考 4.7“认证设置”章节）。如下图所示：

[强制下级组及其用户继承本组认证选项]，可以强制隶属于该用户组的下级用户组及其用户继承本用户组的『认证选项』标签内的所有设置，但是下级用户组能够添加新的认证方式或选择其他外部认证服务器。

通过组合可以有以下的认证方式：

[用户名/密码]＋[短信认证』/[硬件特征码]/[动态令牌]

[数字证书/Dkey 认证]＋[短信认证』/[硬件特征码』/『动态令牌]

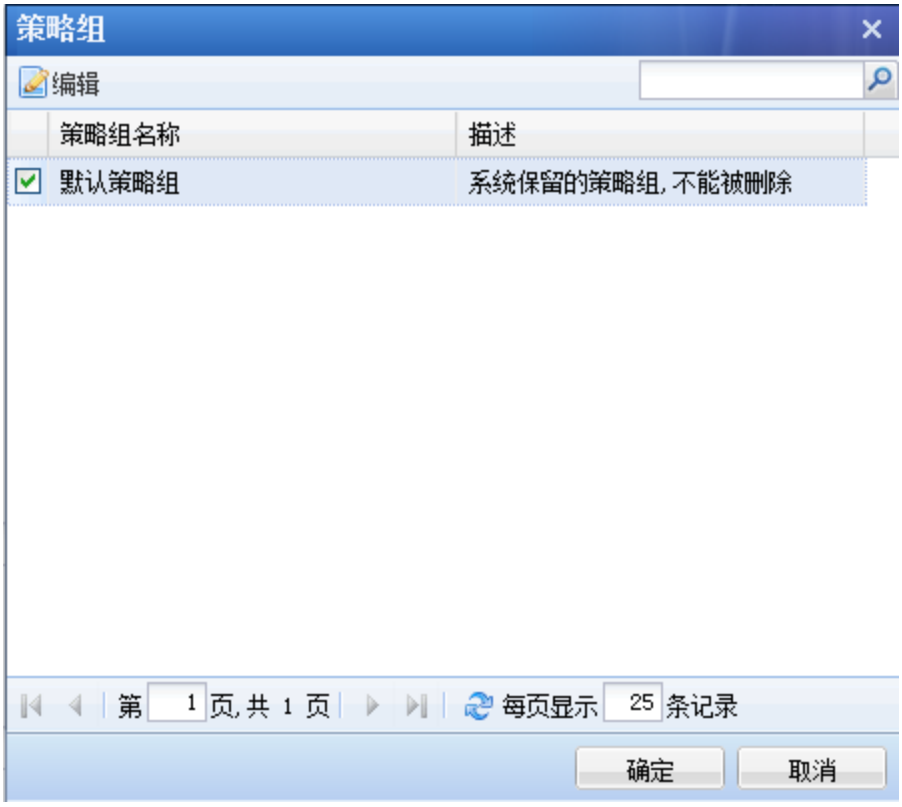
[外部认证]＋[短信认证』/[硬件特征码』/[动态令牌]

[用户名/密码]＋[数字证书/Dkey 认证』＋[短信认证]/[硬件特征码]/[动态令牌]

[外部认证]＋[数字证书/Dkey 认证』＋[短信认证』/[硬件特征码』/[动态令牌]

『接入策略组』用来设置用户使用的各种策略，具体设置可以参考 4.8『策略组管理』章节。

点击  ，弹出【策略组】编辑框，如下图所示：



点击编辑按钮，用来修改选中的策略组。

勾选应用的策略组后，点击确定，如下图所示

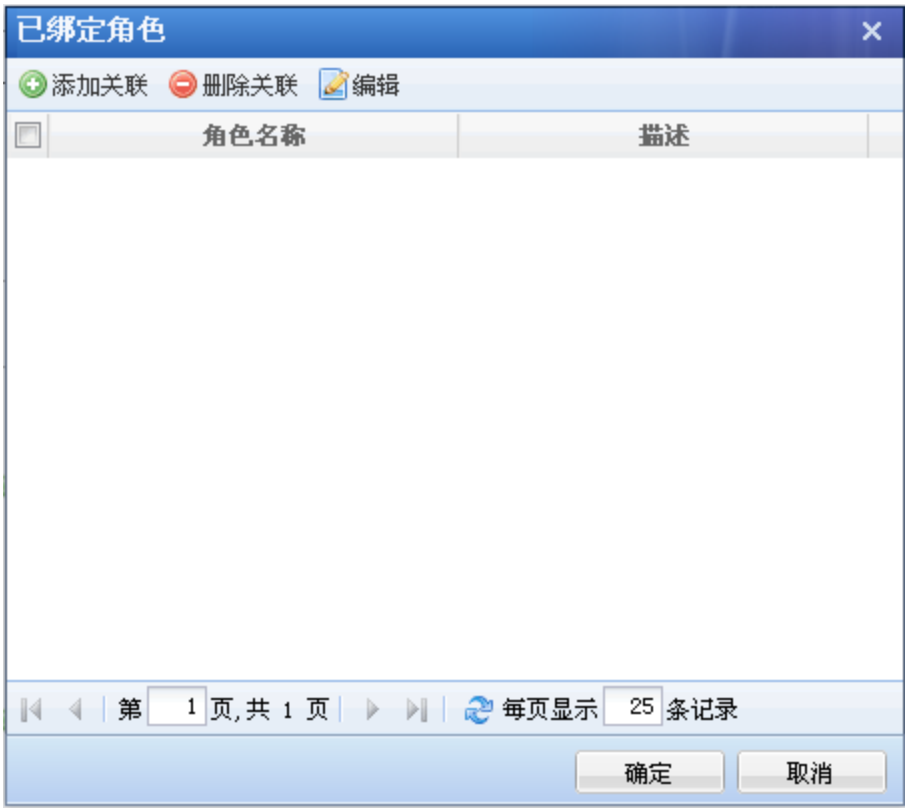
点击新建策略组并选用按钮，打开『新建策略组』对话框编辑新策略，编辑完成点击点击保存按钮，保存该策略并关联给当前用户组。具体设置可以参考 4.8『策略组管理』章节。

[强制下级组及其用户继承本组策略组]，可以强制隶属于该用户组的下级用户组及其用户继承本用户组所关联『接入策略组』标签内的所有设置。

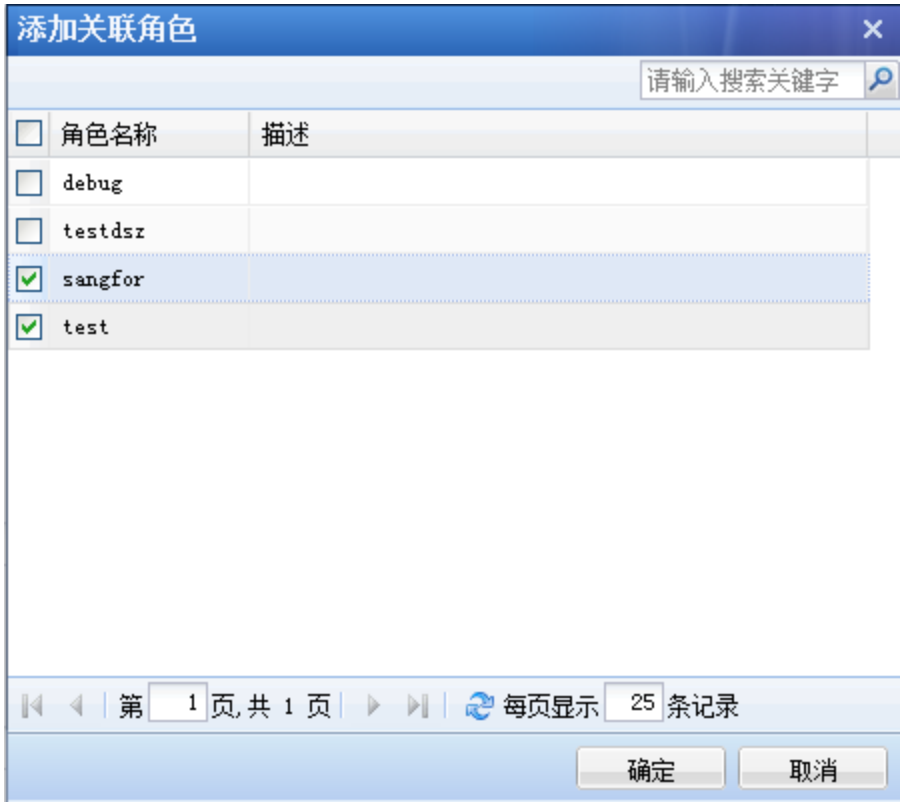
『关联角色』用来选择该用户组所使用的角色，角色的具体设置可以参考 4.6『角色授权』章节。

点击新建角色并关联按钮，打开【新建角色】对话框并编辑新角色，编辑完成点击保存按钮，保存该角色并关联给当前用户组。具体设置可以参考 4.6『角色授权』章节。

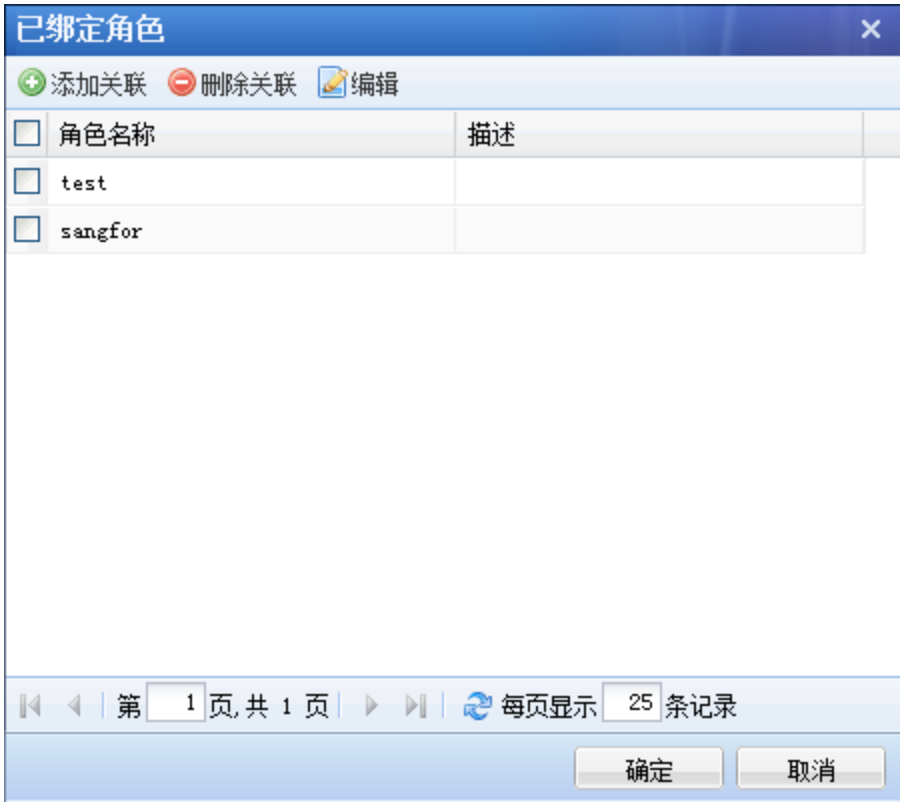
点击 为该用户组选择相应的角色，如下图所示：



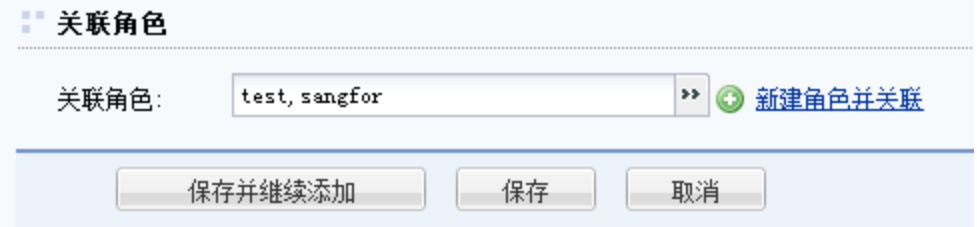
点击添加关联按钮，用来选择需要关联的角色，弹出【添加关联角色】的对话框，如下图所示：



勾选相应的角色，点击确定，如下图所示：



再点击确定，如下图所示：



关联角色成功，该用户组关联了两个角色。

点击保存職继续添加，可继续添加角色。

点击保存按钮，保存配置。

注意：『默认用户组』和『匿名用户组』下不能够新建下级用户组。

4.4.2. 新建用户

WEBUI 路径：『VDI 设置』→『用户管理』。

点击新建，在下拉框中选择用户，弹出『新建用户』的操作界面。

界面如下图所示：

『名称』即 VDI 用户登录 VPN 时所使用的帐号。

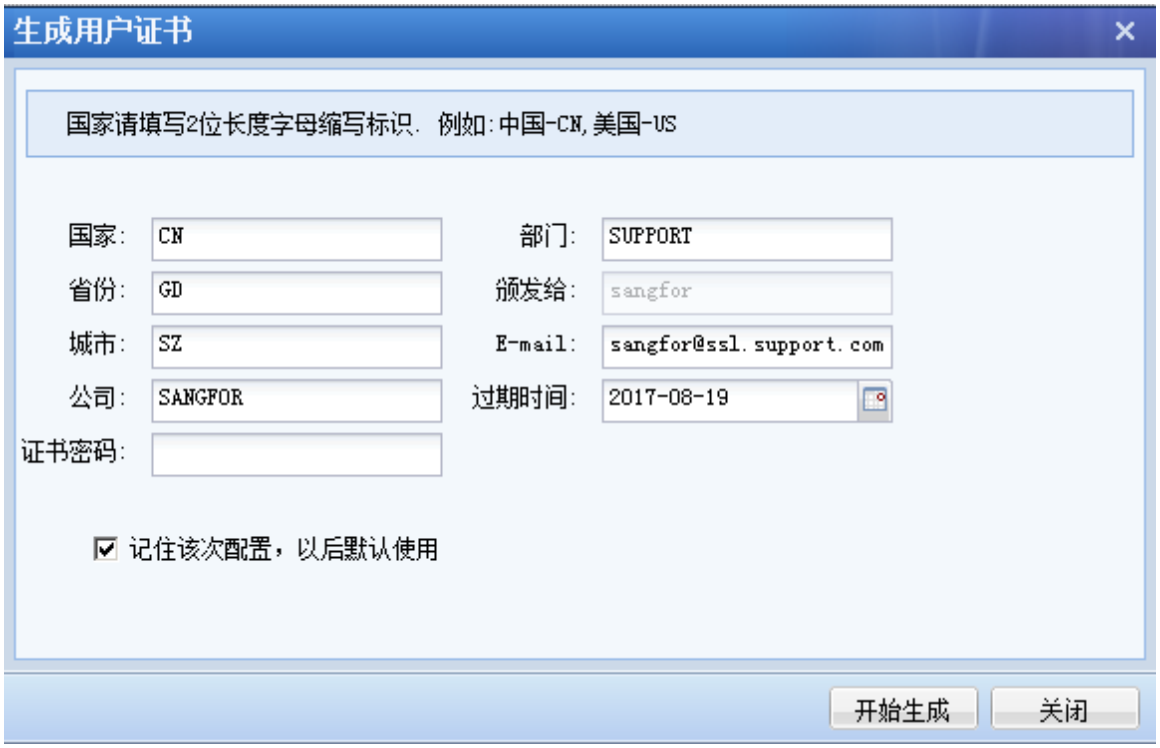
『描述』可任意填写用户的相关说明信息。

『密码』和『确认密码』用于设定 VDI 登录帐号的密码。

『手机号码』用于填写用户的手机号码。如果启用了[短信认证]功能，必须填写。

『生成证书』用于给使用内置数字证书认证的用户生成数字证书。若再『VDI 设置』→『认证设置』→『证书与 USB-KEY 认证』里禁用了内置 CA，将弹出如下提示：

若再『VDI 设置』→『认证设置』→『证书与 USB-KEY 认证』里启用了内置 CA，并设置了内置 CA 的相关选项，点击生成证书按钮，界面如下图所示：

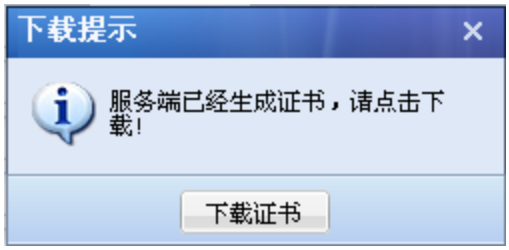


数字证书相关信息中的『国家』、『省份』、『城市』、『公司』、『部门』、『过期时间』、『E-mail』信息存在默认值，可以进行修改。修改后勾选[记住该次配置，以后默认使用]，把当前『证书密码』、『颁发给』除外的所有证书信息作为默认配置保存，后续用户生成数字证书可直接调用该默认配置。

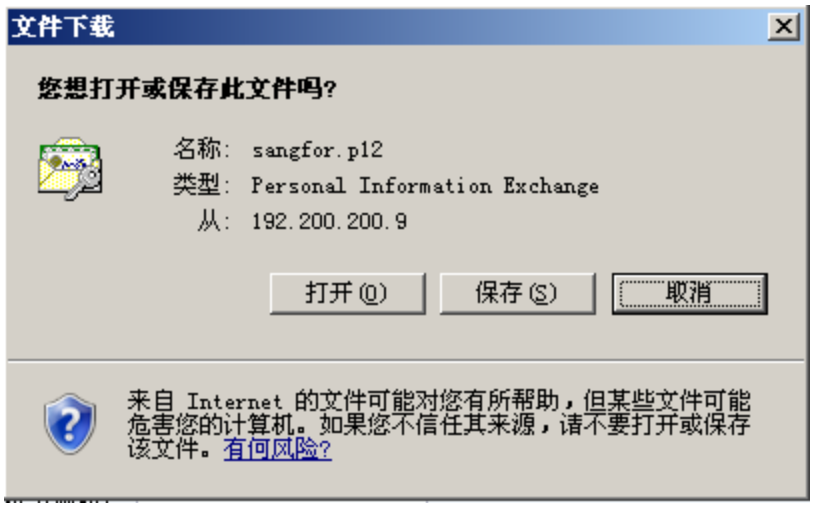
『颁发给』显示的是账户名，只读不可更改。

『证书密码』需根据实际情况填写。在用户导入（安装）数字证书到电脑时需要用到，设定后请告知相应的登录用户。

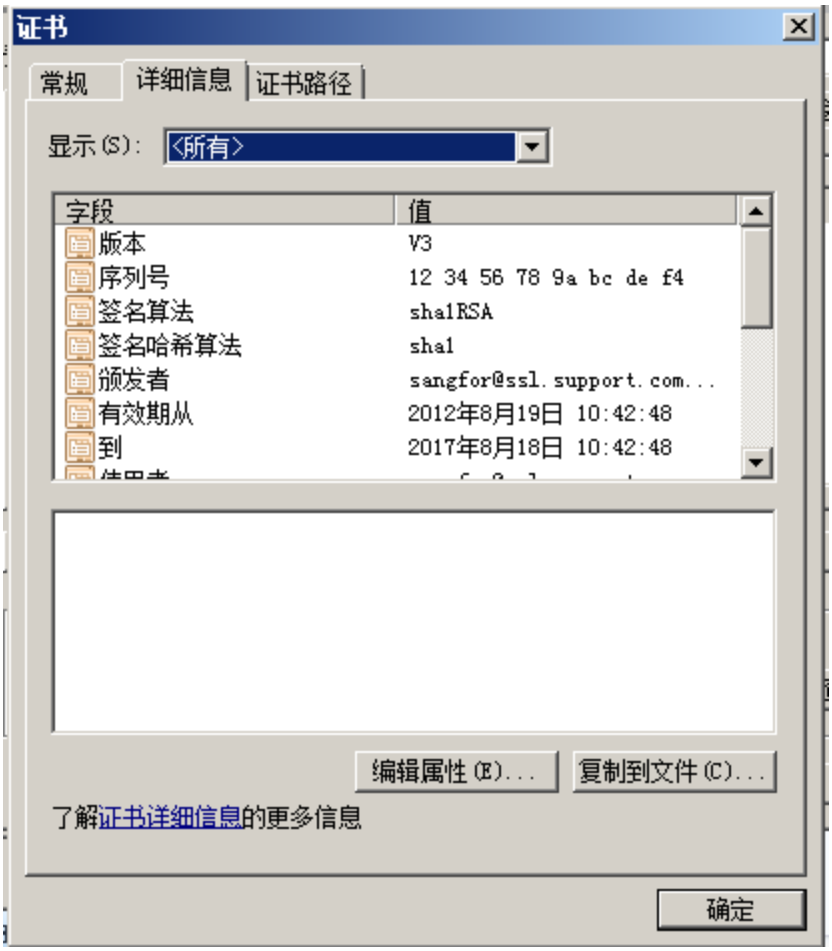
点击开始生成，则开始生成证书，弹出如下图所示对话框：



点击下载证书，选择证书的保存路径，会保存为以“.p12”为后缀的数字证书文件。如下图所示：



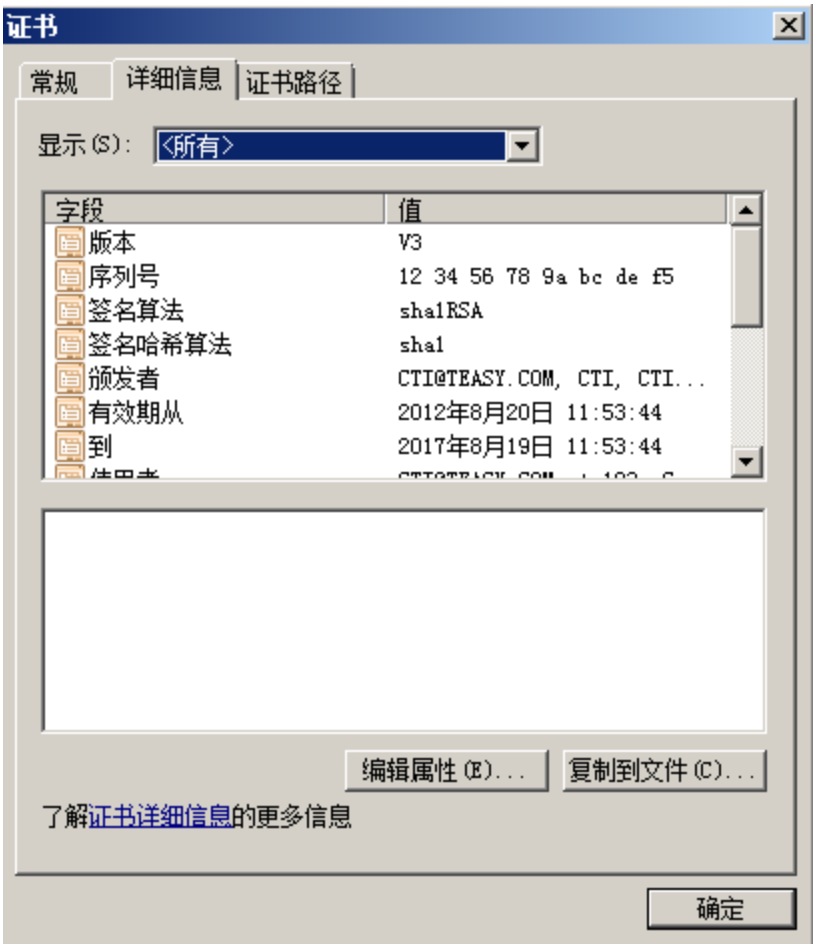
此时，界面上会显示该证书用户的序列号。



『导入证书』用于给使用第三方数字证书认证的用户导入用户证书。点击导入证书按钮，界面如下图所示：

选择相应的证书文件，设置证书密码，选择该用户使用的第三方 CA 证书机构，点击确定保存配置。

此时，界面上会显示该证书用户的序列号。



可以将鼠标移至外置 CA，点击后面的编辑图标，更改用户的绑定字段和所属的外置 CA。

『创建 USB-KEY』用于给使用 DKEY 认证的用户生成 DKEY，可以是有驱 DKEY，也

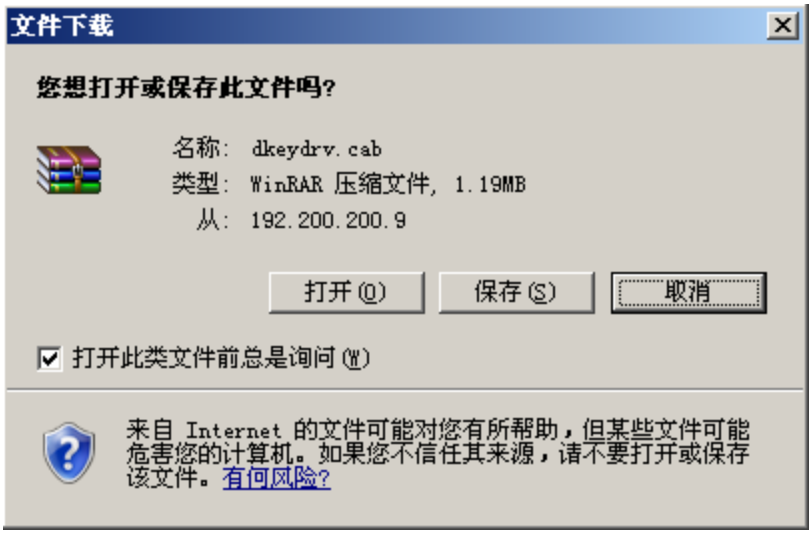
可以是无驱 DKEY。

注意：“生成 USB-KEY”前，必须先安装证书导入控件和 USB-KEY 驱动。

WEBUI 路径：『VDI 设置』→『认证设置』→『主要认证』。

如下图所示：

点击下载安装 USB-KEY 驱动，出现以下界面：

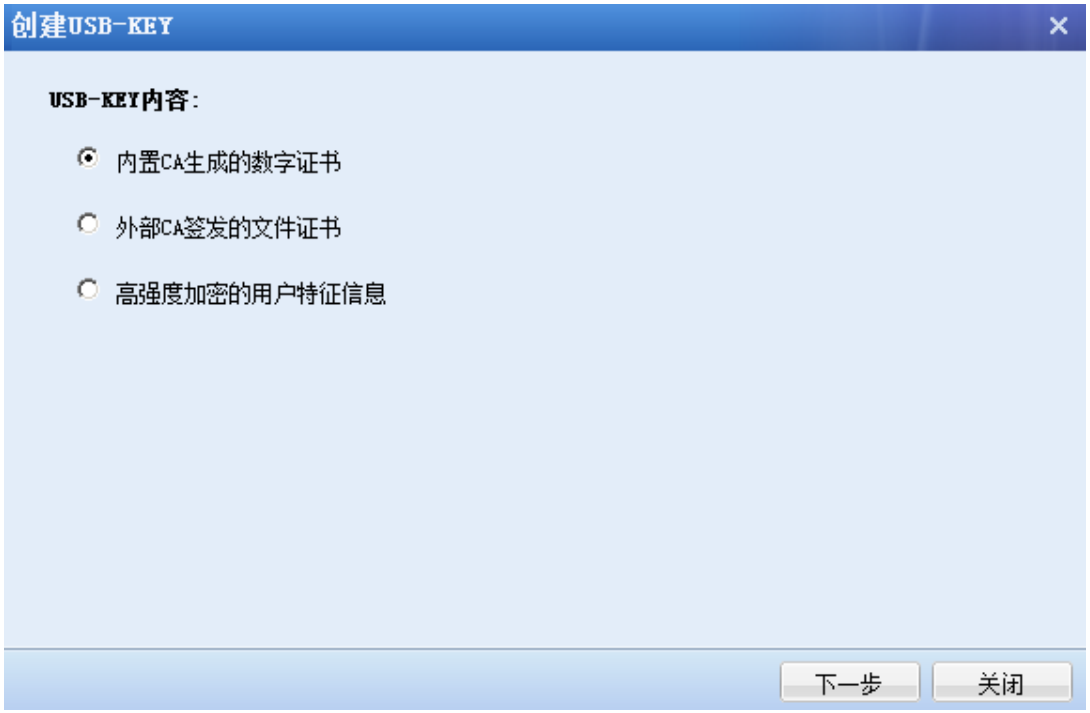


下载后，安装 USB-KEY 驱动。

点击下载安装导入控件，将文件名为“DKeyImport.exe”的安装包下载后，安装完成。

注意：安装证书控件时，必须以系统管理员权限登陆系统才可以完整安装。

点击创建 USB-KEY 按钮，如下图所示：



[内置 CA 生成的数字证书]需要由设备内置 CA 来签发一张证书，并写入 USB-KEY 中。

[外置 CA 签发的文件证书]需要由第三方 CA 来签发一张证书，并写入 USB-KEY 中。

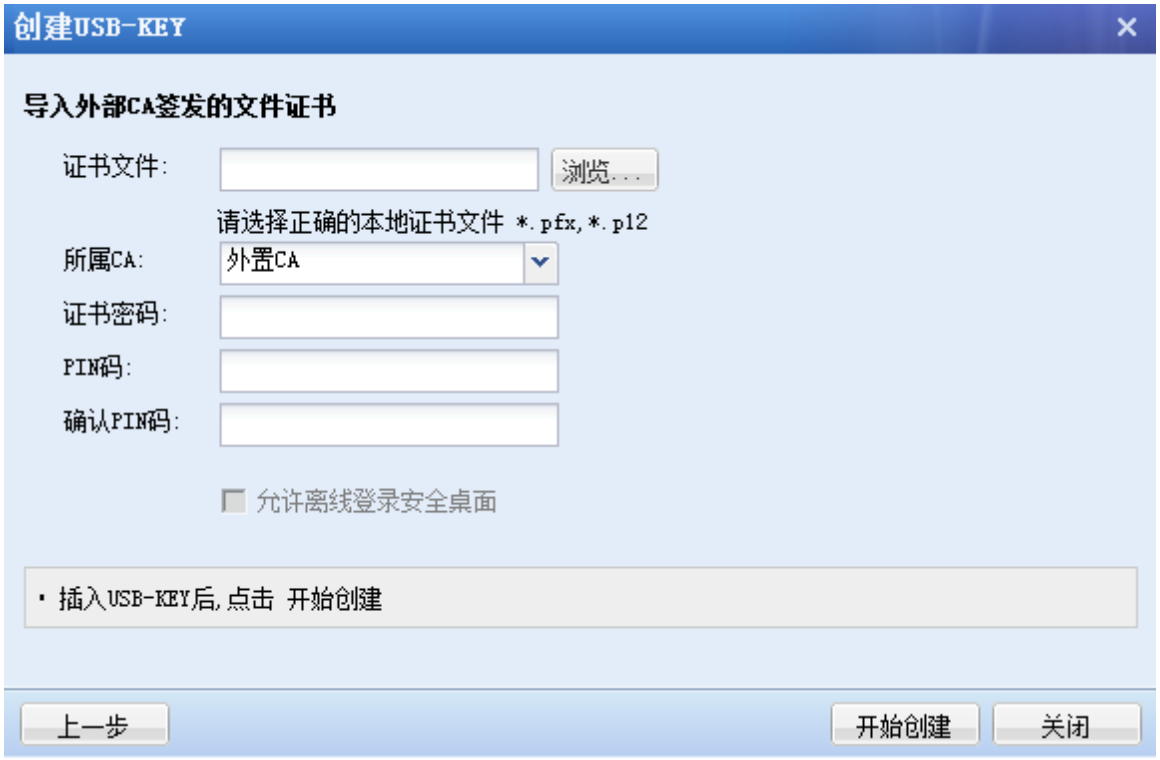
[高强度加密的用户特征信息]中存放的是经高强度加密后的，用来唯一标示该用户的特征信息。登录时，可以根据 USB-KEY 中的信息识别登录用户的身份。

选择[内置 CA 生成的数字证书]，点击下一步，如下图所示：

输入 DKEY 的 PIN 码，插入 USB-KEY，点击开始创建，生成证书成功。

注意：若用户关联了离线访问安全桌面的策略且用户认证 DKEY 和离线登录安全桌面的 DKEY 是同一个 DKEY，还需要勾选上“允许离线登录安全桌面”。

选择[外置 CA 签发的文件证书]，点击下一步，如下图所示：



输入证书密码和 DKEY 的 PIN 码，插入 USB-KEY，点击开始创建，生成证书成功。

注意：若用户关联了离线访问安全桌面的策略且用户认证 DKEY 和离线登录安全桌面的 DKEY 是同一个 DKEY，还需要勾选上“允许离线登录安全桌面”。

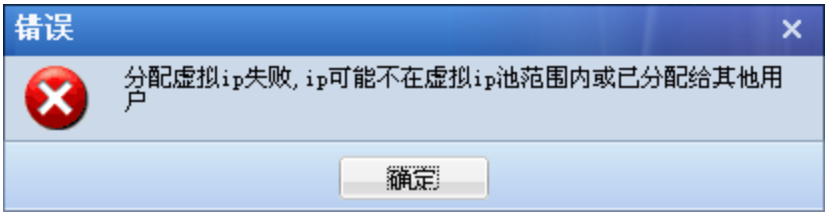
选择[高强度加密的用户特征信息]，点击下一步，如下图所示：

输入 DKEY 的 PIN 码，插入 USB-KEY，点击开始创建，生成证书成功。

注意：若用户关联了离线访问安全桌面的策略且用户认证 DKEY 和离线登录安全桌面的 DKEY 是同一个 DKEY，还需要勾选上“允许离线登录安全桌面”。

『虚拟 IP』将虚拟 IP 和“当前用户”绑定。可以选择[自动获取]或[手动设置]。

如果选择[自动获取]，则用户登录后自动从虚拟 IP 池中分配一个虚拟 IP；如果选择[手动设置]，则可以点击获取空闲 IP 按钮，在后面方框中自动出现可以绑定的虚拟 IP；当然也可以手动填写虚拟 IP 地址，如果填写的虚拟 IP 不在虚拟 IP 池内，或者被其他用户绑定，那么在点击保存按钮后，会出现如下提示框：



注意：只有“私有用户”才可以绑定虚拟 IP，

“用户”可以单独设置认证方式，缺省情况下“用户”自动继承所在“用户组”的认证方式等属性。

『过期时间』，包括[永不过期]和[手动设置]两种。

若勾选[永不过期]则该用户一直都可以使用；

若勾选[手动设置]，则在后面的方框中选择日期，如果到了这个时间，那么该用户将被禁用。

『账号状态』，可选择[启用]或[禁用]。

若勾选[启用]则该账号可以正常使用；

若勾选[禁用]，则该账号被禁用，无法使用。

『所属组』可设定该用户属于哪个用户组。

『离线访问』若用户关联了离线访问安全桌面的功能，可以将用户与离线访问安全桌面的 DKEY 进行绑定，则该用户在离线状态下，只能使用指定的 DKEY 访问安全桌面。

点击绑定 USB-KEY，弹出如下提示：

勾选[继承所属组认证选项和策略组]，当前用户自动关联上级用户组认证选项和接入策略组。

勾选[继承所属接入策略组]，当前用户继承上级用户组的接入策略。

勾选[继承所属组认证选项]，当前用户继承上级用户组的认证策略。

不勾选[继承所属组认证选项和策略组]则当前用户可以独立设置认证方式和接入策略。

『认证选项』和『接入策略组』、『关联角色』标签内的设置项和【新建用户组】页面的一样，此处不再赘述。

完成配置后，点击保存，最后在『用户管理』页面点击配置生效，保存配置并生效。

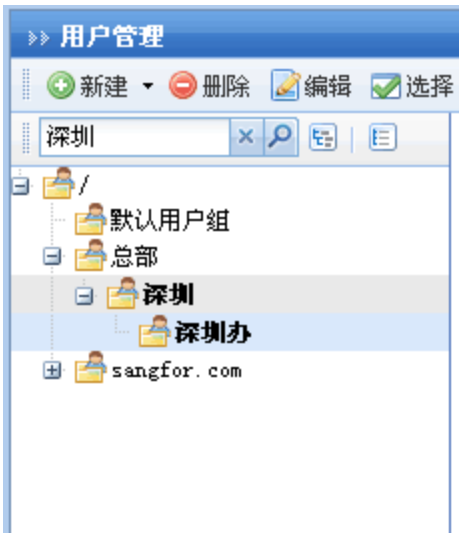
4.4.3. 高级搜索

位于界面右上方的搜索框，可[按名称]、[按描述]、[按虚拟 IP]或[按手机号码]来搜索用户，在后面的方框可填入需要搜索的具体内容，点击放大镜图标，会直接显示相关用户的相关信息。

点击高级搜索按钮，如下图所示：

可以根据包含关键字、关键字类型、搜索范围、认证类型、过期时间、闲置时间来查询相应的用户。

位于用户组织结构上方的搜索框，可以查找有相应关键字的用户组，如下图所示：



点击用户列表中『名称』标签，即可对用户、用户组进行升降序排列。

点击『列』标签，可根据下拉表的选项进行显示列的筛选，如下图：

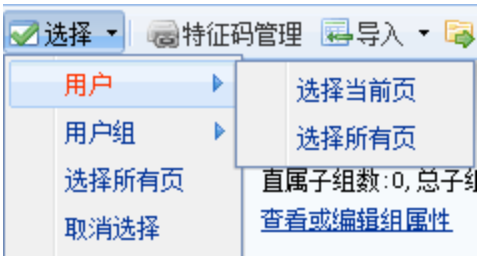
点击『类型』标签，可以选择列出不同类型的用户，方便管理，如下图所示：

点击『类型』、『描述』、『其他信息』、『状态』等标签后的，即可对用户/用户组进行升降序排列。

在【用户管理】界面勾选用户（组），然后点击删除按钮即可批量删除用户（组）。

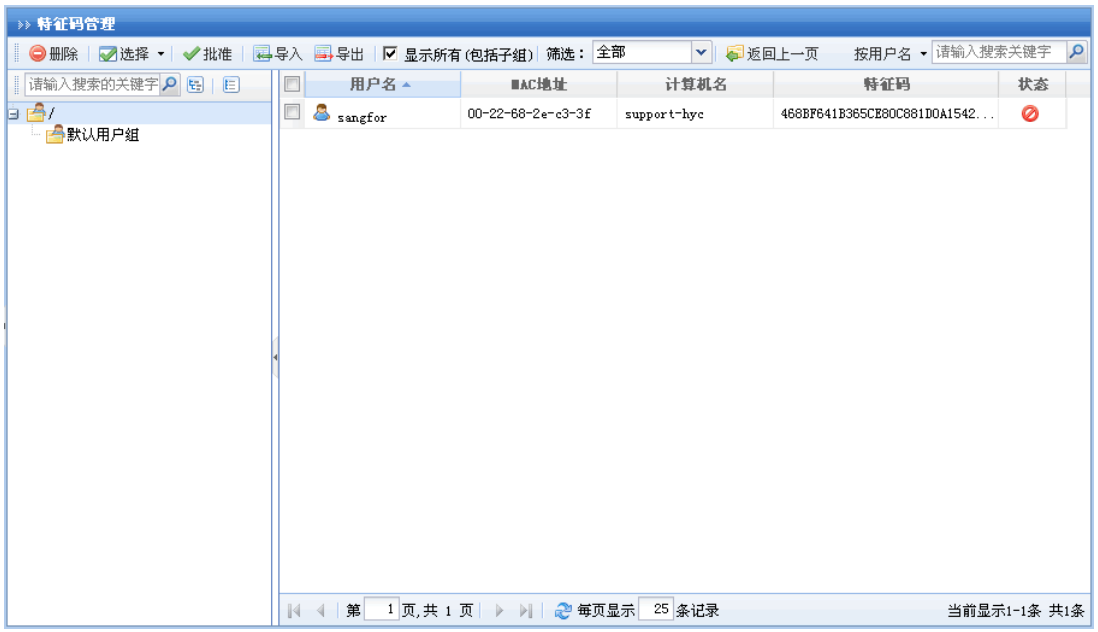
勾选好某个目标用户（组），点击编辑按钮，可进入用户（组）信息编辑页面，对目标用户（组）进行修改。

点击选择按钮，可以按照用户、用户组选择显示当前页或者所有页上的用户。也可以取消选择，如下图：



4.4.4. 特征码管理

点击特征码管理按钮，进入【特征码管理】配置页面，如下图所示：

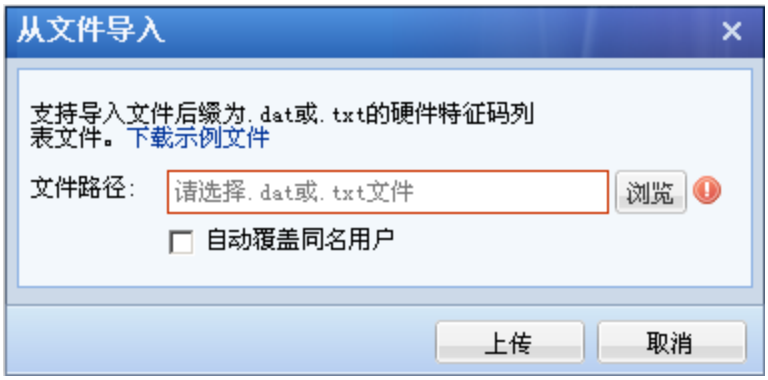


勾选用户，点击删除按钮即可批量删除用户特征码。

点击选择按钮，可以选择所有用户的特征码或者取消选择。

勾选用户，点击批准按钮即可批量审批用户特征码。

点击导入按钮，则手动导入用户的硬件特征码，如下图所示：

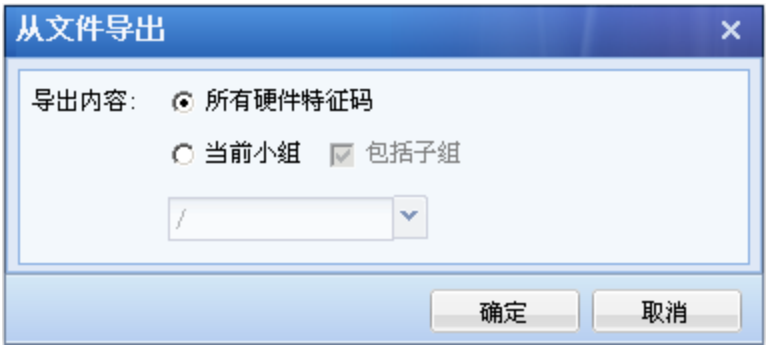


点击下载示例文件按钮，可以根据里面的示例格式来编写特征码文件。

勾选[自动覆盖同名用户]，则从文件导入特征码会自动覆盖列表中已有的同名用户的特征码。

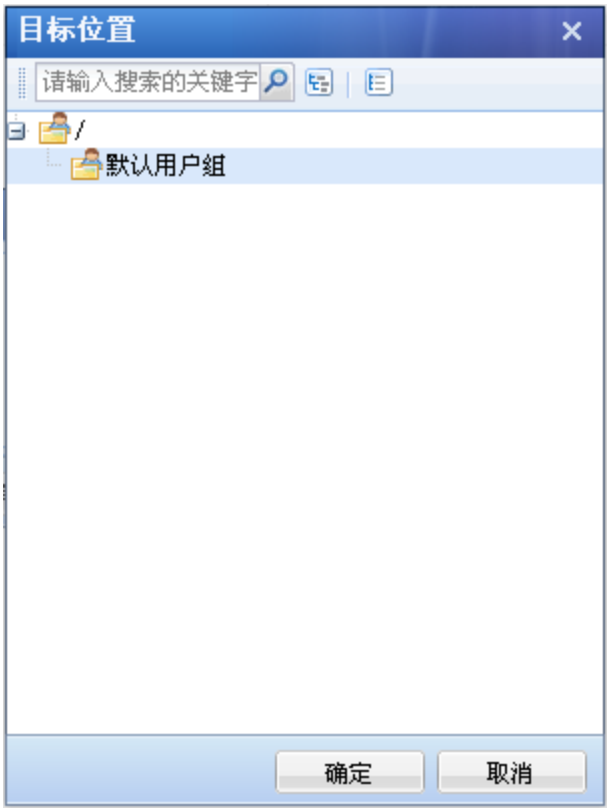
点击浏览按钮，选择编辑好的特征码文件，点击上传按钮即可。

点击导出按钮，则手动将列表中的硬件特征码导出到文件中，如下图所示：

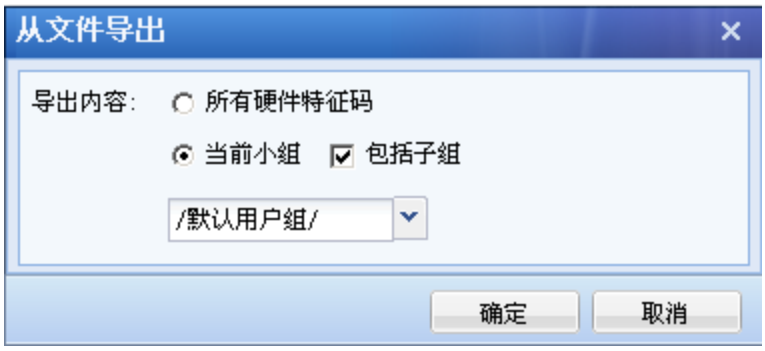


选择[所有硬件特征码]，则点击确定按钮，将列表中所有用户特征码全部导出到文件中。

选择[当前小组]，点击下拉框，如下图所示：

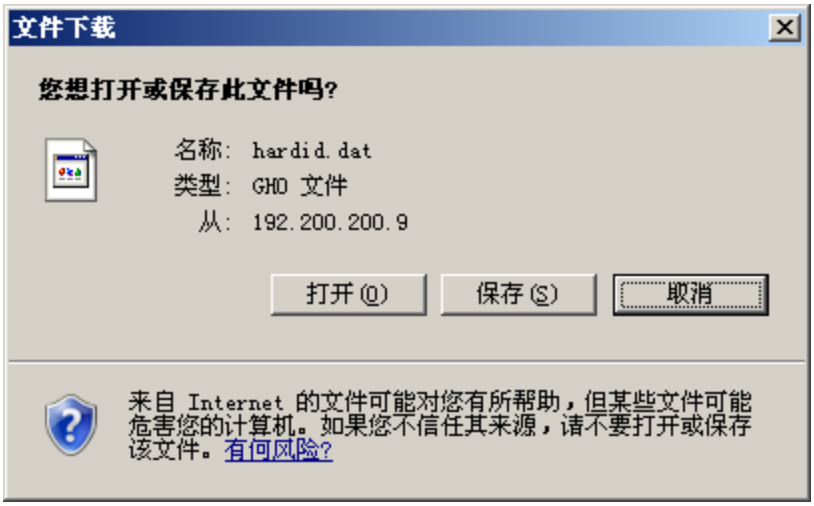


点击导出硬件特征码的用户组，点击确定按钮，如下图所示：



点击确定按钮，则将选定用户组中的用户的特征码导出到文件中。

如下图所示：



若勾选了[包括子组]，则选定用户组的子组所属用户的特征码也同样被导出。

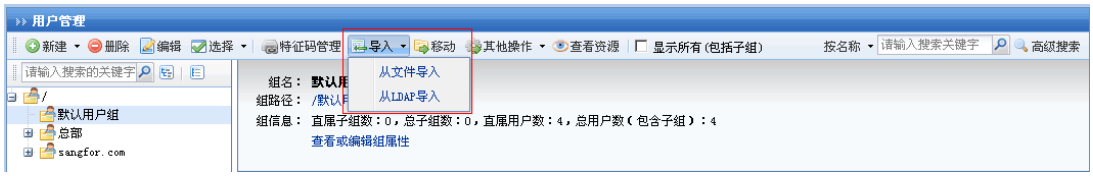
勾选[显示所有（包括子组）]，则在列表中显示所有用户的硬件特征码，否则只显示当前用户组所属用户的硬件特征码。

在『筛选』中，可以分别选择显示[全部]、[已审批]、[未审批]的硬件特征码。

页面右上角的搜索，可以选择[按用户名]或[按计算机名]来搜索相应的硬件特征码。

4.4.5. 导入用户

『用户管理』中的『导入』分[从文件导入]和[从 LDAP 导入]两种。



第一种：选择[从文件导入]，如下图所示：

若选择[从文件中（*.csv）导入用户]，如下图所示：

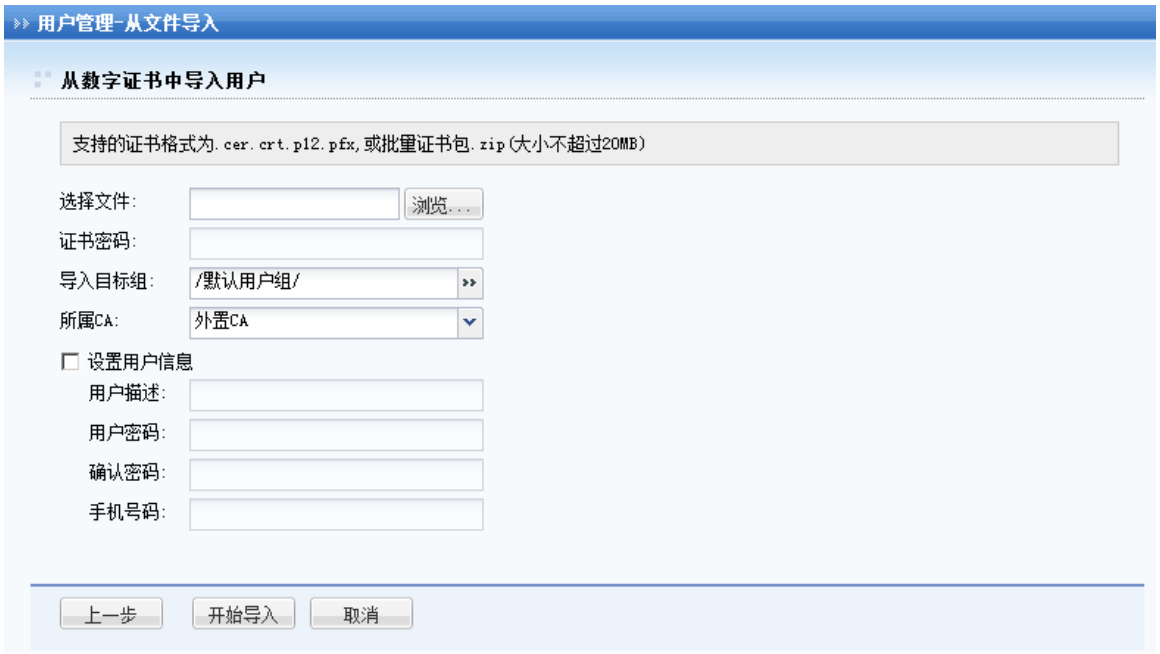
可以通过 csv 文件批量导入用户的账号，支持“用户名”、“所属组路径”、“描述”、“密码”、“手机号码”、“虚拟 IP 地址”等信息的导入，其中“用户名”为必填项，其他均为选填项，点击下载示例文件，查看编写导入文件的格式。

勾选[未指定用户组的用户导入到]，在下拉框中选择用户组，那么没有在文件中指定用户组的用户就会被导入到该用户组中。

勾选[用户所属组不存在时，自动创建]，如果在本地没有该用户组就会自动创建新用户组；对于本地已存在的用户，若选择继续导入并覆盖已存在用户时，当所导入用户列表中的用户账号和设备用户列表中的原有用户名字冲突（相同），新导入的用户信息会覆盖原有的用户信息；若选择跳过，则不导入该用户。

选择编辑好的文件，点击下一步，完成。

若选择[从数字证书中导入用户]，如下图所示：



可通过 cer、crt、p12、pfx 后缀的数字证书或批量证书包导入证书用户的账号。

『证书密码』，如果证书有密码，需要填写证书密码。

『导入目标组』选择导入证书用户所属的用户组。

『所属 CA』选择导入证书用户所属的 CA。

勾选[指定用户信息]，需要填写『用户描述』、『用户密码』、『确认密码』、『手机号码』。，导入的证书用户会继承相应的信息。不勾选将采用默认配置，属于默认用户组，描述、密码、手机号码默认为空。

若选择[从文件中（*.xml）导入组织结构]，如下图所示：

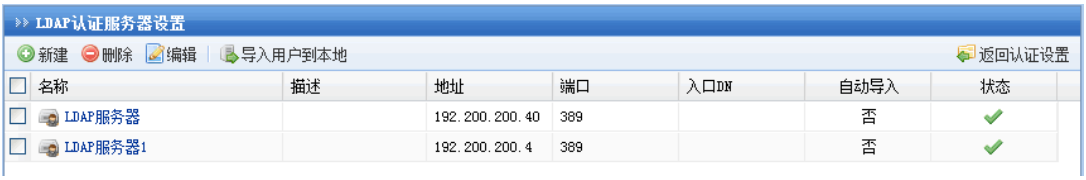
『选择文件』中选择编辑好的文件。

点击下载示例文件按钮，可以查看编写格式。

『导入目标组』选择将组织结构导入到当前某个用户组下。

第二种：选择[从 LDAP 导入]，从 LDAP 服务器中导入相应的用户、用户组等信息。

如下图所示：



点击新建，弹出重新建立一个 LDAP 服务器的界面，具体设置可以参考 4.4『认证设置』中的『LDAP 认证模块』设置。

勾选列表中的 LDAP 服务器，点击删除，则可以单个或者批量删除 LDAP 服务器。

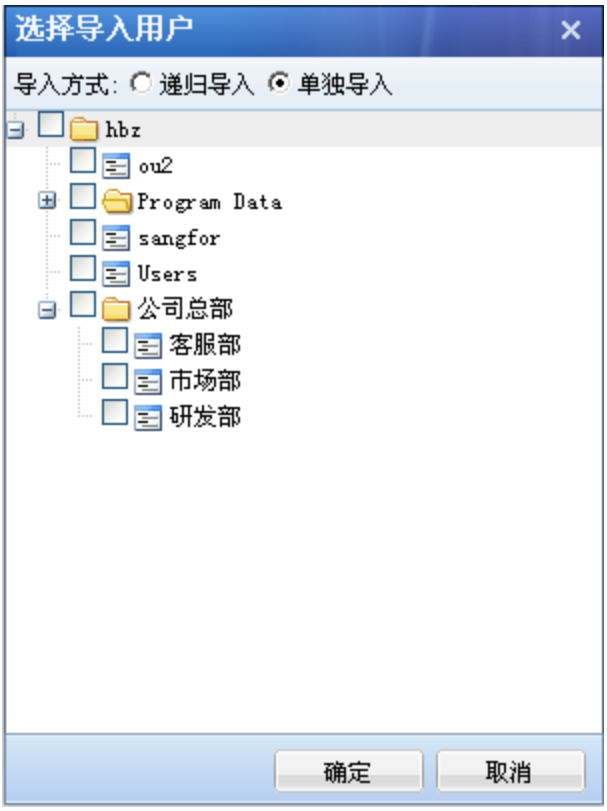
勾选列表中的 LDAP 服务器，点击编辑，则可以编辑所选择的 LDAP 服务器。

勾选列表中的 LDAP 服务器，点击导入用户到本地，如下图所示：

『从此 LDAP 服务器导入』显示当前选择的 LDAP 服务器的名称。

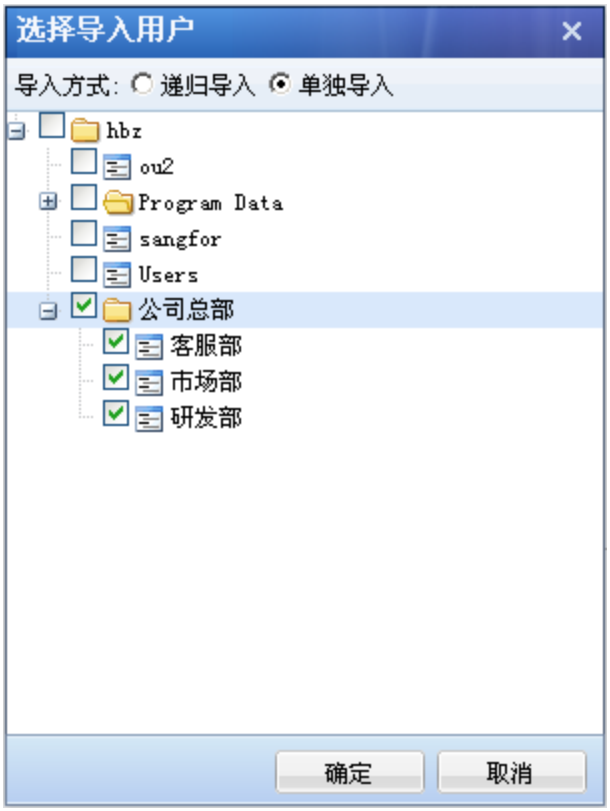
『选择导入用户』显示当前要导入到用户管理列表中的 LDAP 服务器中的用户。

点击选择导入用户，如下图所示：

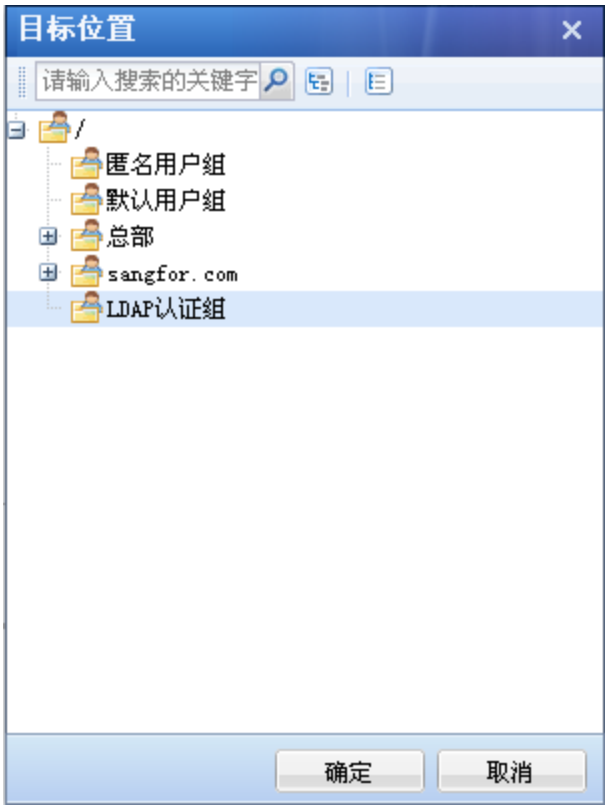


『导入用户』分为两种方式：[递归导入]和[单独导入]。

第一种：选择[单独导入]，勾选需要导入的 LDAP 用户组，如下图所示：



『选择导入到的本地目标组』选择要把 LDAP 中的用户导入到哪个用户组，如下图所示：

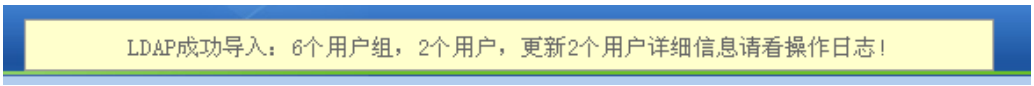


『导入方式』分两种: [复制 LDAP 上的组织结构到目标位置，并导入用户到相应组中]和[所有用户都导入到目标组，忽略 LDAP 上的组织结构]。

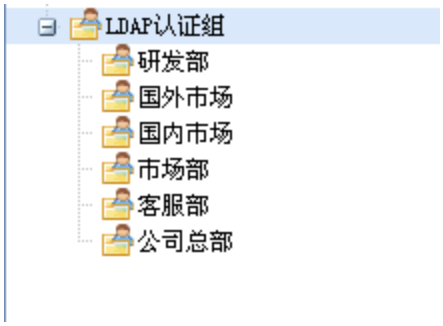
若选择[复制 LDAP 上的组织结构到目标位置，并导入用户到相应组中]，那么将用户导入的同时，即可将勾选中的几个 OU 同步到所选的本地用户组中。

设置完成后，如下图所示：

点击保存并立即同步，如下图所示：



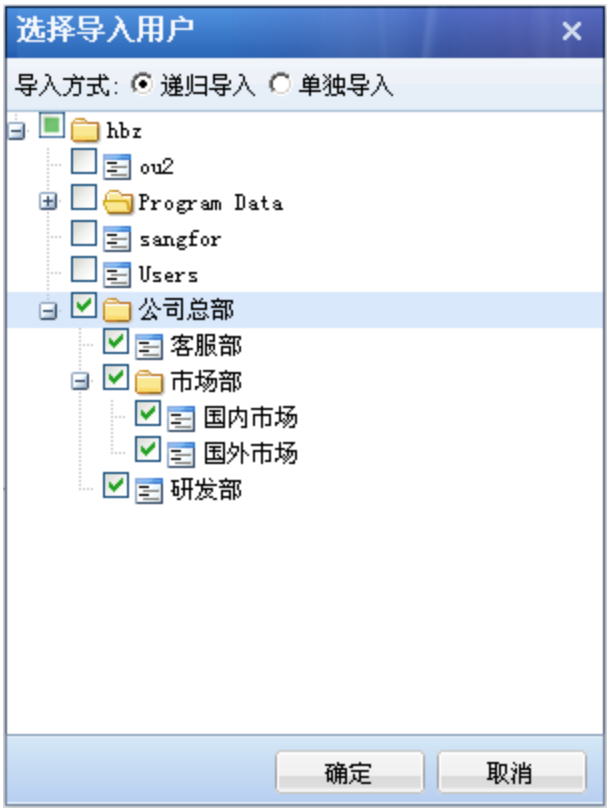
导入成功后，效果如下图所示：



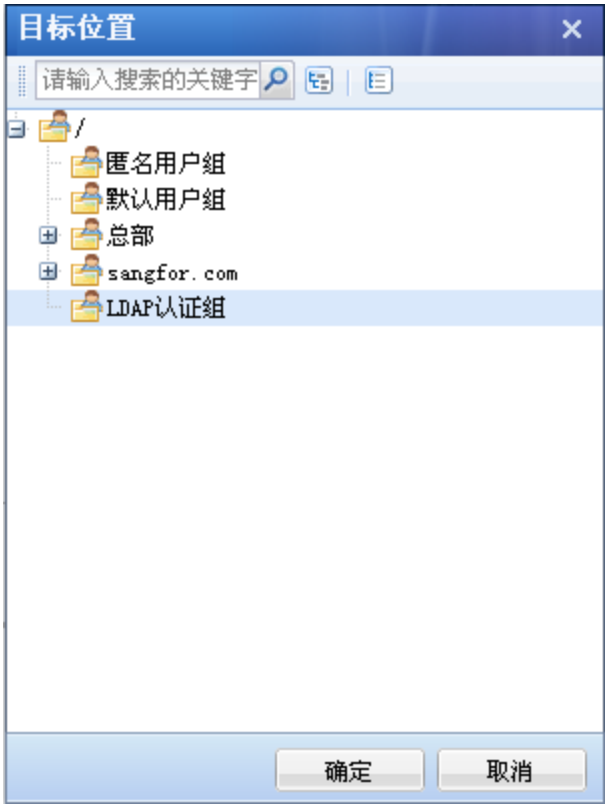
若选择[所有用户都导入到目标组，忽略 LDAP 上的组织结构]，那么就只会将 OU 中的用户导入到指定的本地组中。

第二种：[递归导入]是将 LDAP 中的用户组及其用户按照域中的组织结构导入。

选择[递归导入]，勾选需要导入的 LDAP 用户组，如下图所示：



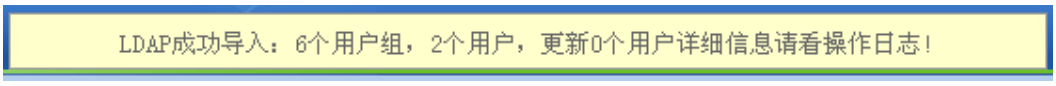
在『选择导入到的本地目标组』中选择要把 LDAP 中的用户导入到哪个用户组，如下图所示：



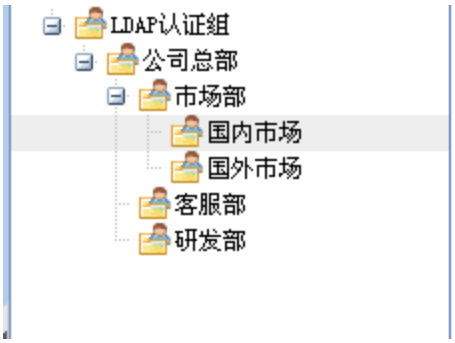
若选择[复制 LDAP 上的组织结构到目标位置，并导入用户到相应组中]，那么将用户导入的同时，即可将勾选中的几个 OU 以及它们之间的组织结构关系同步到所选的本地用户组中。

设置完成后，如下图所示：

点击保存并立即同步，如下图所示：



导入成功后，效果如下图所示：



若选择[所有用户都导入到目标组，忽略 LDAP 上的组织结构]，那么就只会将 OU 中

的用户导入到指定的本地组中。

『本地已经存在的用户』有两种处理方式：[继续导入，覆盖已经存在的用户]和[忽略该用户，不导入本地已存在的用户]。

勾选[继续导入，覆盖已经存在的用户]，若本次导入的用户账号和本地已经存在的用户账号同名，则直接覆盖原有账号。

勾选[忽略该用户，不导入本地已存在的用户]，若本次导入的用户账号和本地已经存在的用户账号同名，则直接忽略该用户，不导入本地。

『自动导入设置』，可以把 LDAP 服务器内所有用户账号自动导入到 VDI 本地用户列表，在设备上生成同名的用户。

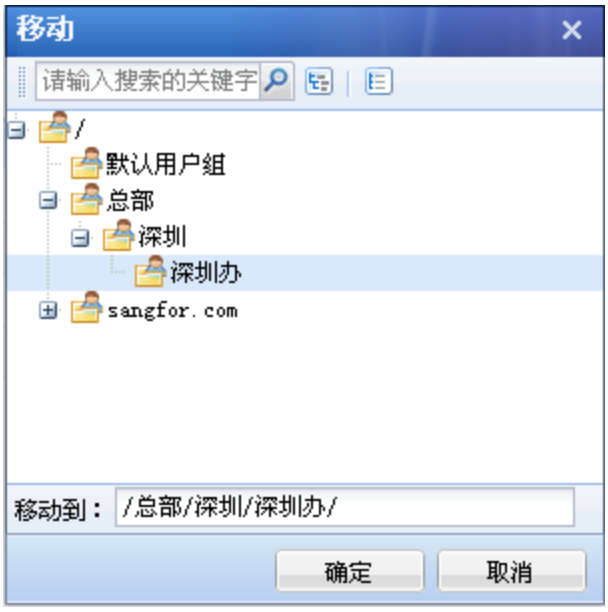
勾选启[用自动导入]，在『自动导入时间间隔』中可以选择“每隔 X 分钟自动导入”或者“定时导入”。点击操作日志可以查看自动导入的结果。

如下图所示：

自动导入可以同时导入用户和用户组。

『用户管理』中的『移动』功能，可以将列表中选定的用户或用户组移动到其他用户组，

如下图所示：



选择想要移动到的目标用户组，点击确定按钮，那么在用户管理列表中选定的用户或用户组就会移动到该用户组。

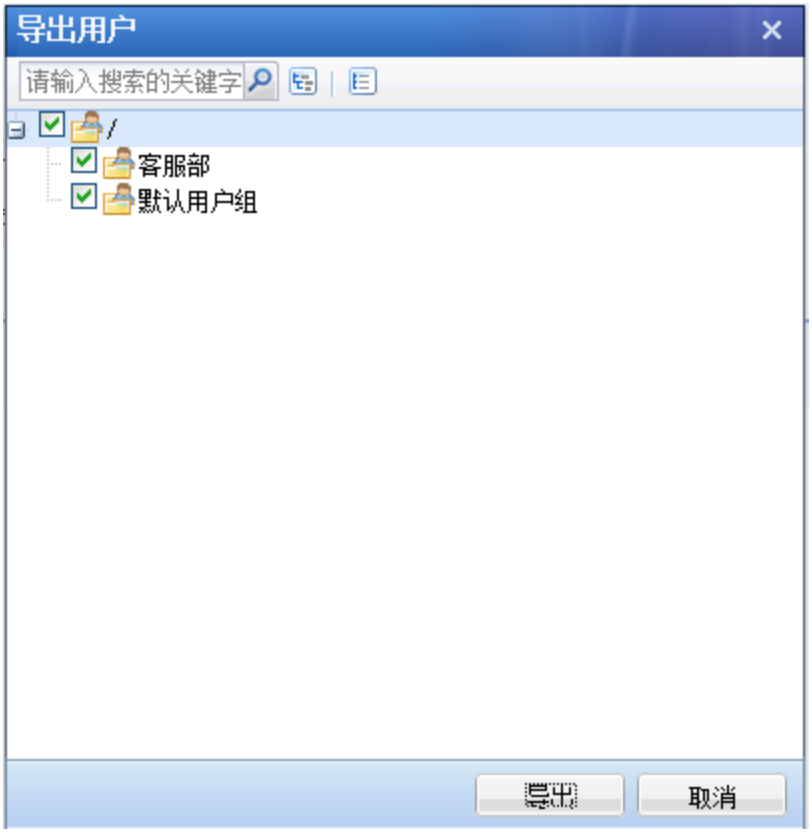
4.4.6. 其他操作

『用户管理』中的『其他操作』功能，包括[导出]、[绑定角色]、[从账号设置]、[批量生成证书]、[批量指定 CA]、[批量创建 USB-KEY]。

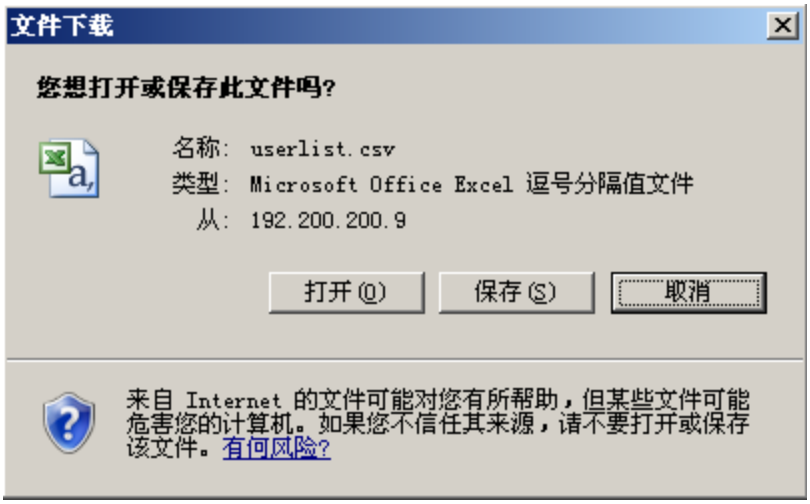
4.4.6.1. 导出

点击导出按钮，如下图所示：

点击选择导出内容按钮会显示出所有的用户组，如下图所示：



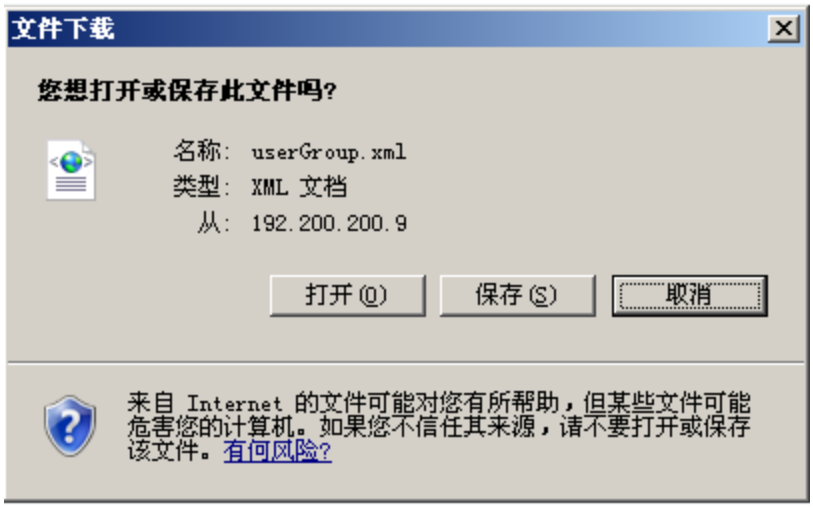
勾选需要导出的用户组，点击导出按钮，即可导出后缀为 csv 的文件，如下图所示：



导出信息包含所勾选的用户组中用户的用户名，所属用户组，密码（经过深信服公司研发的私有算法加密），手机号码，虚拟 IP，描述，最近一次登录信息，如下图所示：

A	B	C	D	E	F	G
#用户名	所属组路径	密码	手机号码	虚拟IP地址	描述	最近一次登陆
zj	/默认用户组	{ 197fba71256ab35f3 }				2011/11/17 3:01
sangfor	/	{ 197fba71256ab35f3 }				2011/11/17 21:12
liushiqin	/	{ 197fba71256ab35f3 }				2011/11/17 1:48
testdsz	/	{ 197fba71256ab35f3 }				2011/11/17 2:09
debug	/	{ 197fba71256ab35f3 }				2011/11/17 19:53
xxl	/	{ 197fba71256ab35f3 }				2011/11/17 20:15
xxl1	/客服部	{ 197fba71256ab35f3 }				从未登陆

点击导出组织架构按钮，即可导出所勾选的用户组所构成的组织架构，如下图所示：

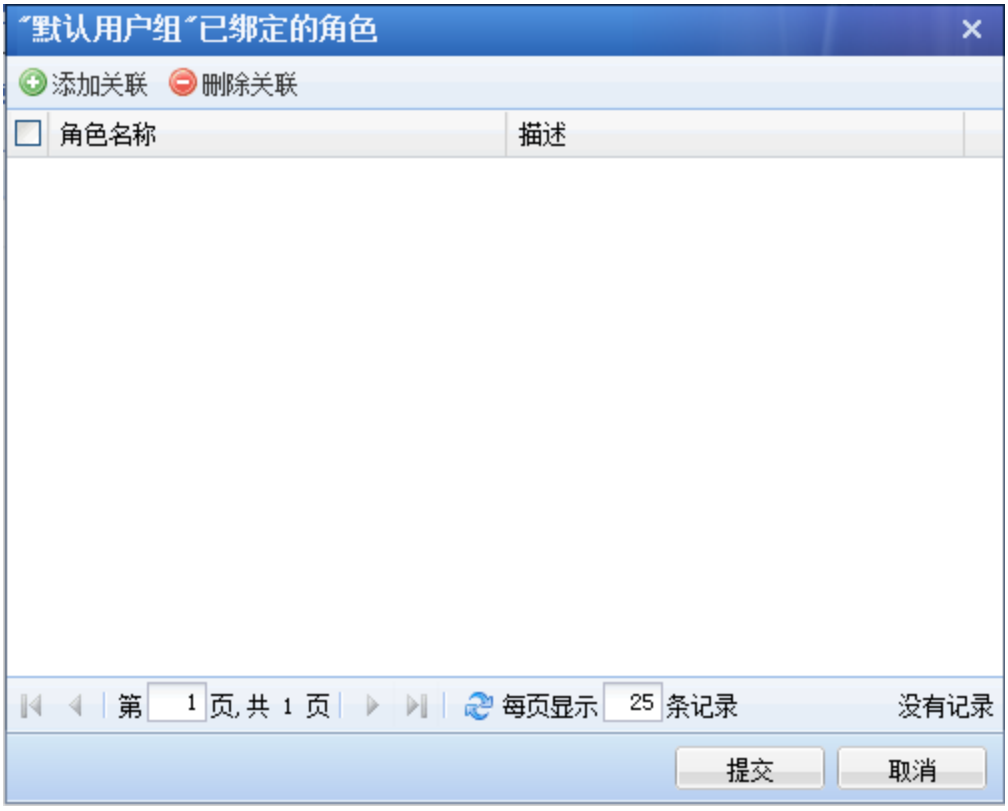


文件打开后显示组织结构信息，如下图所示：

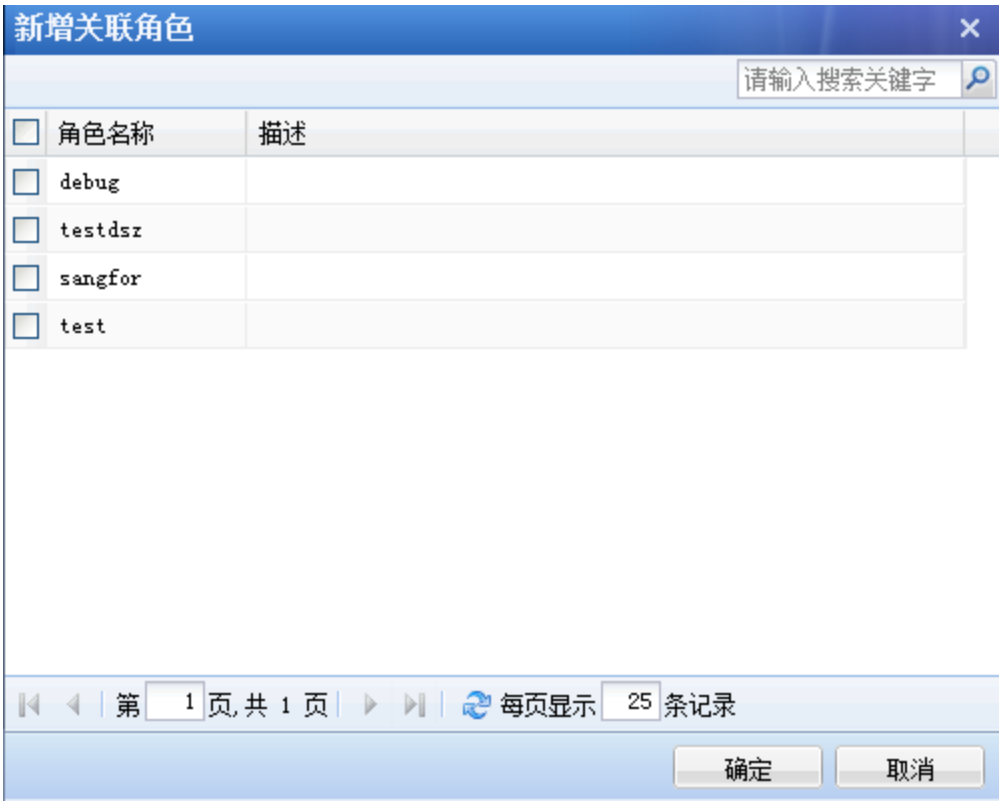
```
<?xml version="1.0" encoding="utf-8" ?>
- <root>
  - <node name="总部" note="">
    - <node name="深圳" note="">
        <node name="深圳办" note="" />
      </node>
    </node>
  - <node name="sangfor.com" note="">
    - <node name="ou2" note="LDAP组映射自动生成用户组">
        <node name="ou4" note="LDAP组映射自动生成用户组" />
      </node>
    - <node name="ou1" note="LDAP组映射自动生成用户组">
        <node name="ou3" note="LDAP组映射自动生成用户组" />
      </node>
    </node>
    <node name="LDAP认证组" note="" />
  </root>
```

4.4.6.2. 绑定角色

在『用户管理』列表中选择用户或用户组，点击绑定角色按钮，在此处可以给用户或用户组关联角色，如下图所示：



点击添加关联按钮，会显示出所有在『角色授权』中定义的角色，如下图所示：



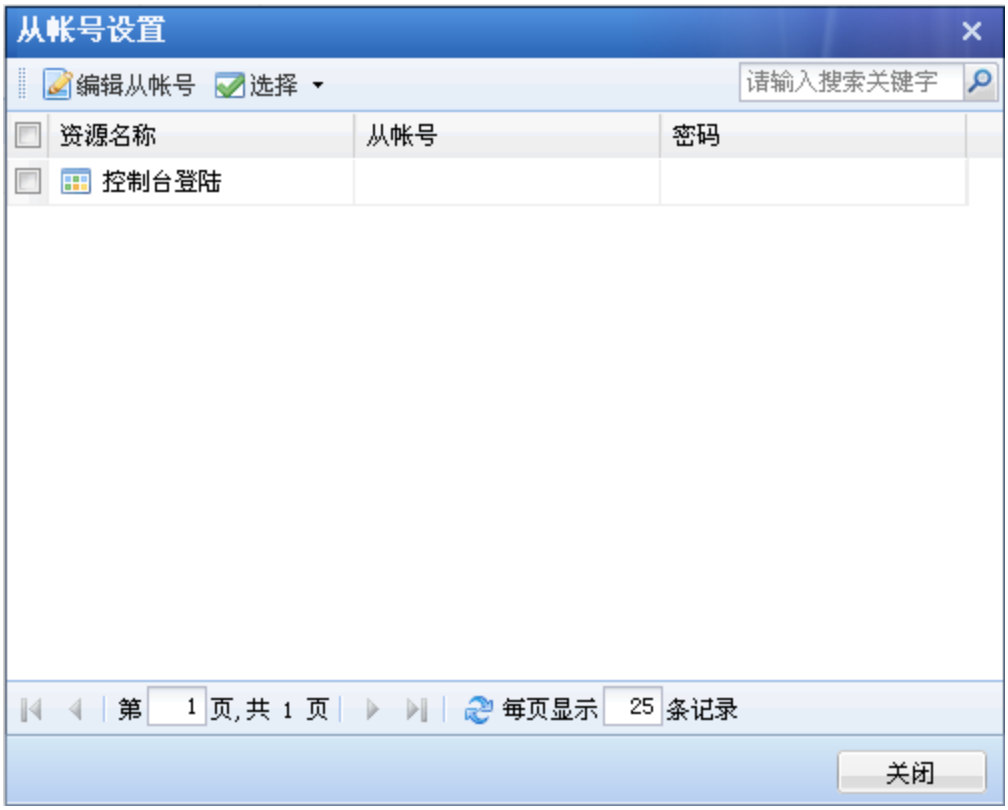
勾选角色，点击确定按钮，给用户绑定角色成功，如下图所示：

点击提交按钮，保存配置。

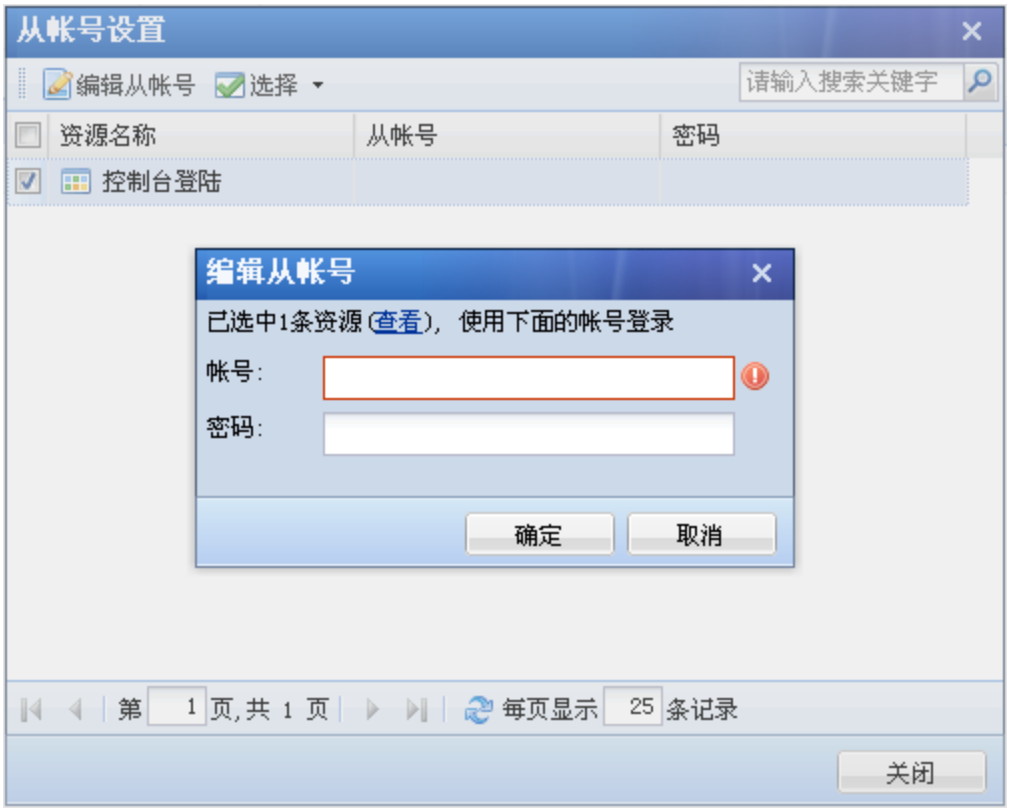
4.4.6.3. 从账号设置

[从账号设置]当用户使用启用了单点登录的资源时，用来设置登录应用系统的账号和密码。当用户点击单点登录资源的时候，VDC 设备自动提交从账号设置的账号和密码。

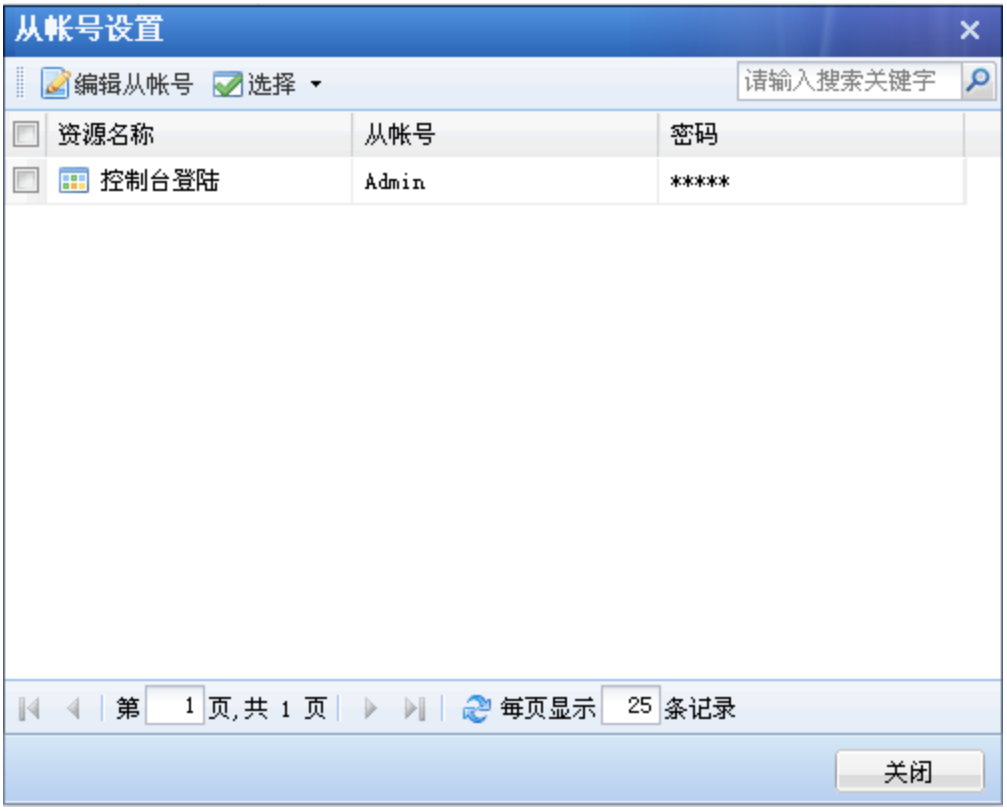
勾选关联了单点登录资源的用户，选择[从账号设置]，弹出【从账号设置】对话框，如下图所示：



勾选资源，点击编辑从账号按钮，如下图所示：



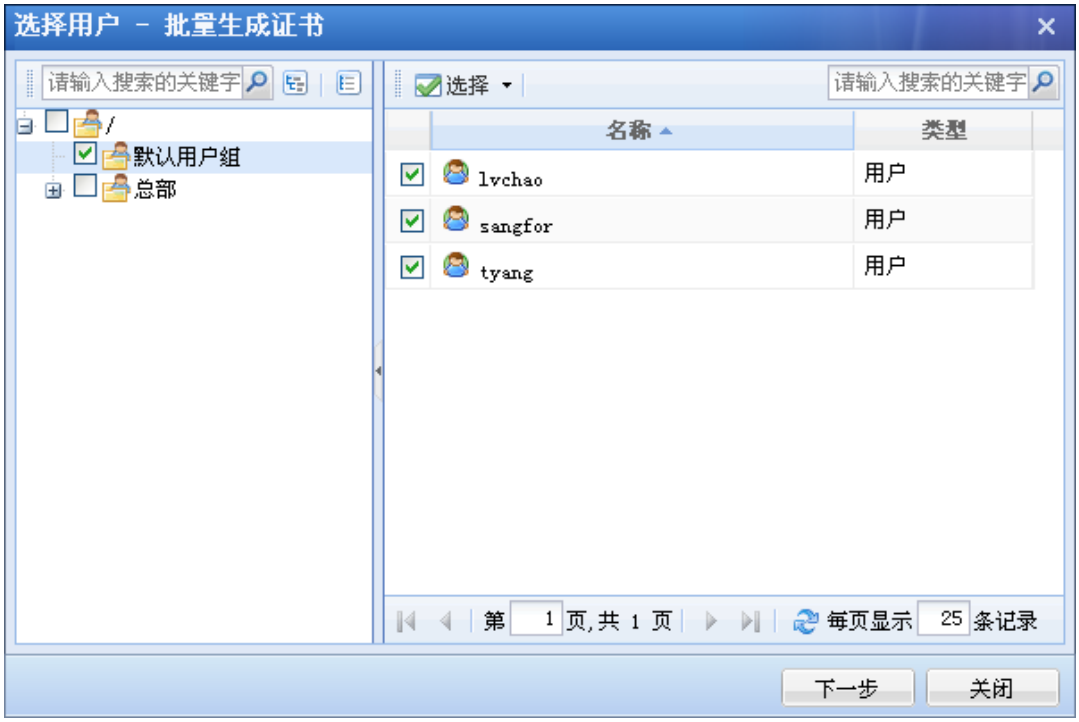
在【编辑从账号】对话框中填写正确的账号和密码，点击确定按钮，如下图所示：



点击关闭按钮，完成设置，并点击配置生效按钮，保存配置。

4.4.6.4. 批量生成证书

点击批量生成证书按钮，可以同时为多个用户生成证书，如下图所示：

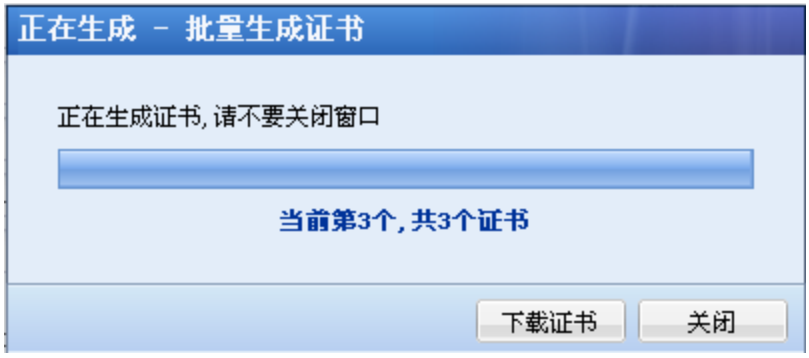


勾选需要生成证书的用户，点击下一步，如下图所示：

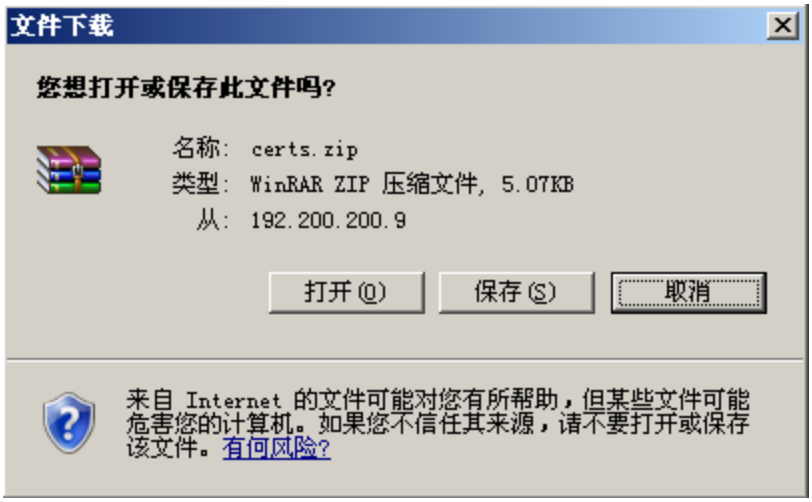
数字证书相关信息中的『国家』、『省份』、『城市』、『公司』、『部门』、『过期时间』信息存在默认值，可以修改，修改后点击记住该次设置，以后默认使用，把当前

『证书密码』、『颁发给』除外的所有证书信息作为默认配置保存。后续用户生成数字证书可直接调用该默认配置。其中『颁发给』和『E-mail』信息无法编写。『颁发给』显示的是与用户名相同。

点击开始生成按钮，按照次序一次生成用户证书，如下图所示：

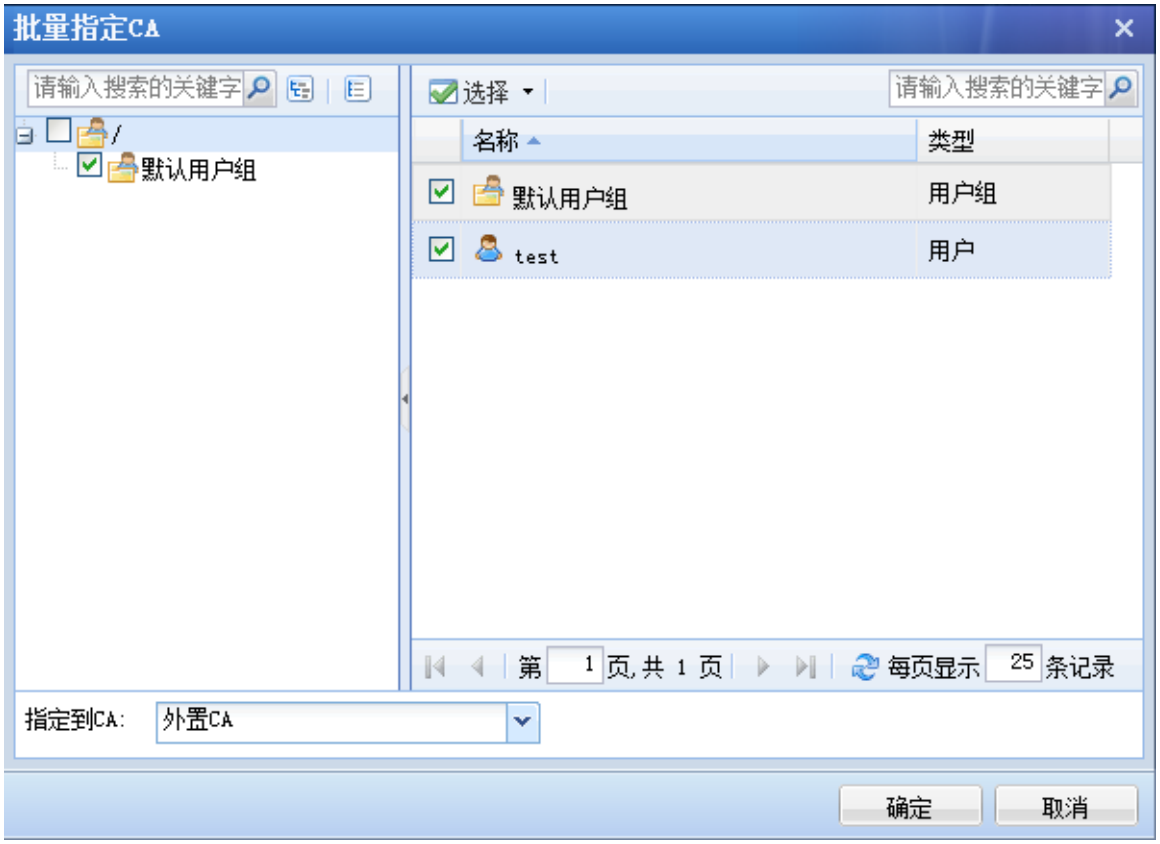


点击下载证书按钮，将生成的证书保存下来，如下图所示：



4.4.6.5. 批量指定 CA

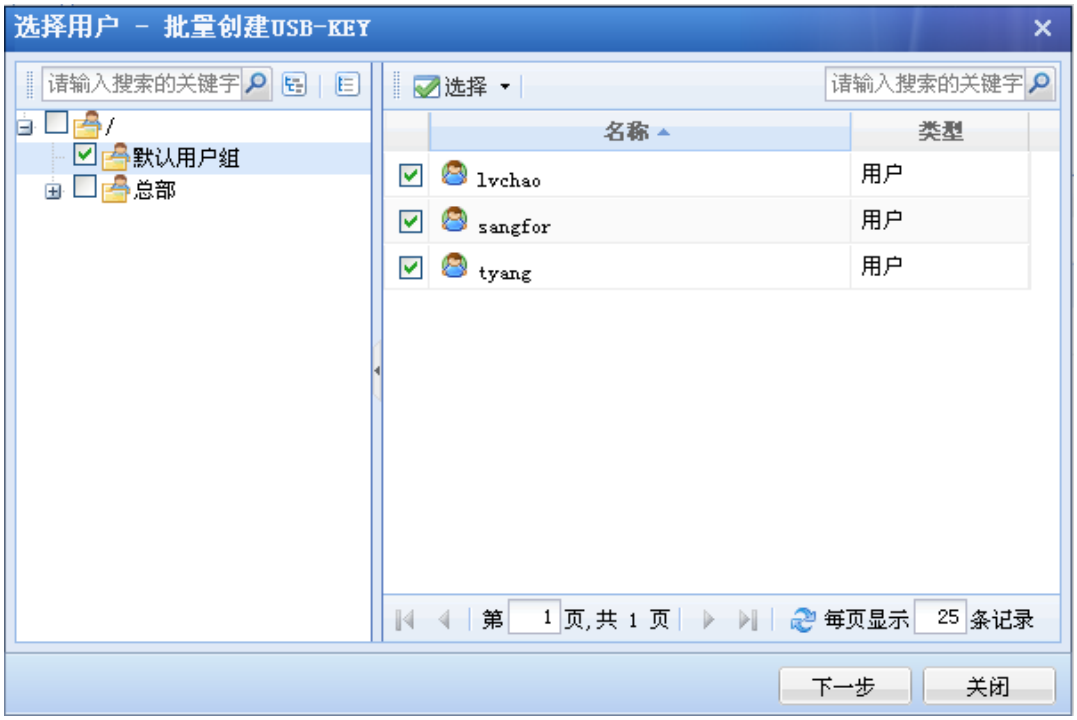
点击批量指定 CA 按钮，可以同时为多个用户指定所属的第三方 CA，如下图所示：



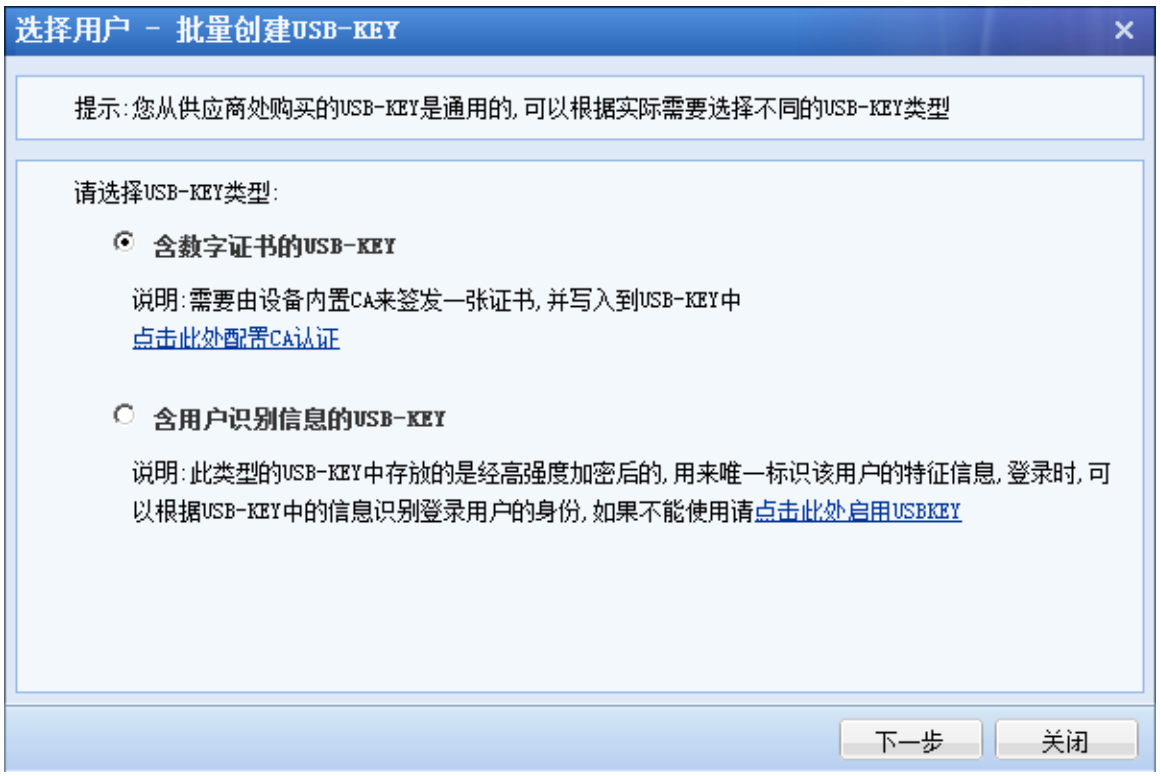
勾选需要指定 CA 的用户，然后选择指定到某个 CA，点击确定。

4.4.6.6. 批量创建 USB-KEY

点击批量创建 USB-KEY 按钮，可以同时给多个用户生成 USB-KEY，如下图所示：

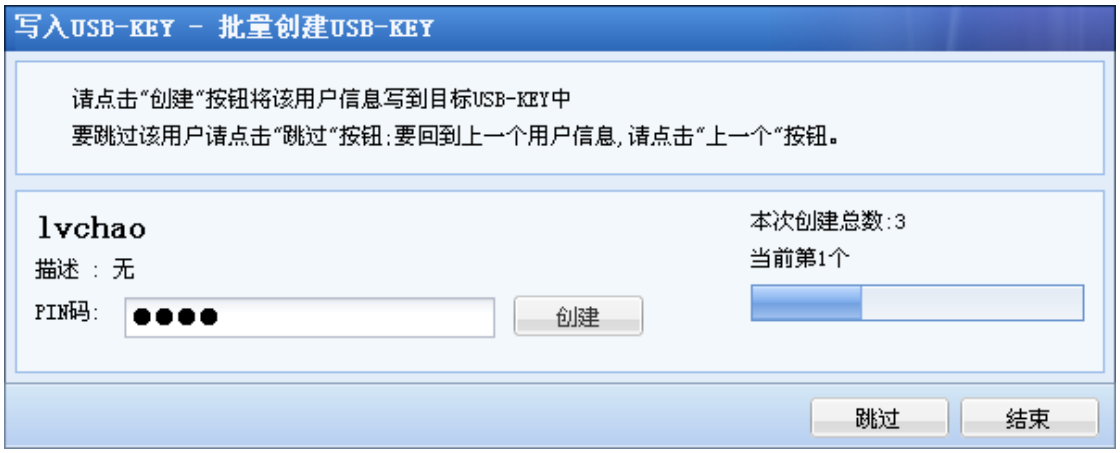


点击下一步，如下图所示：



点击下一步，如下图所示：

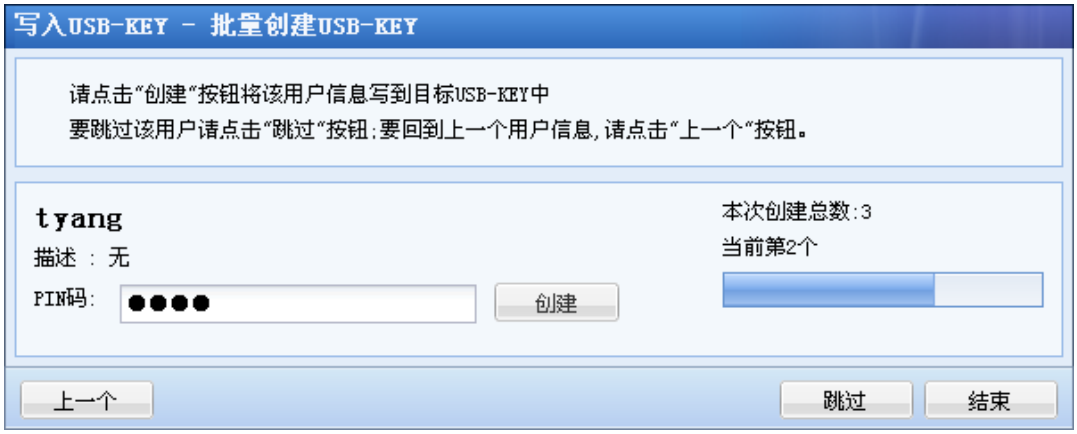
填入默认 PIN 码，点击开始创建，如下图所示：



插入 USB-KEY，点击创建按钮，开始创建证书，将该用户信息写到目标 USB-KEY 中，然后再开始生成下一个用户的 USB-KEY。

如果某一个用户不需要生成 USB-KEY，要跳过该用户请点击跳过按钮。

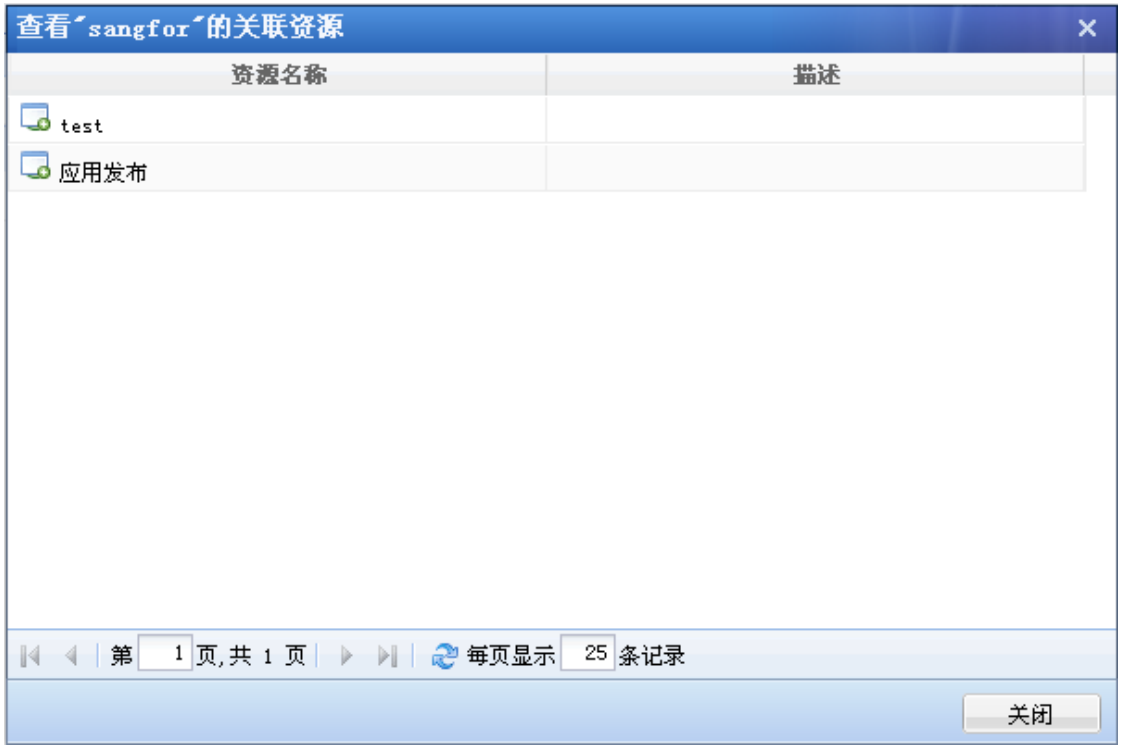
如果要回到上一个用户信息，请点击上一个按钮，如下图所示：



如果需要停止设置生成 USB-KEY，则点击结束按钮。

4.4.7. 查看资源

在『用户管理』选择某一个用户或用户组，点击查看资源按钮，则会显示所关联的资源，如下图所示：



上图中显示用户“sangfor”关联了两个资源“test”和“应用发布”。

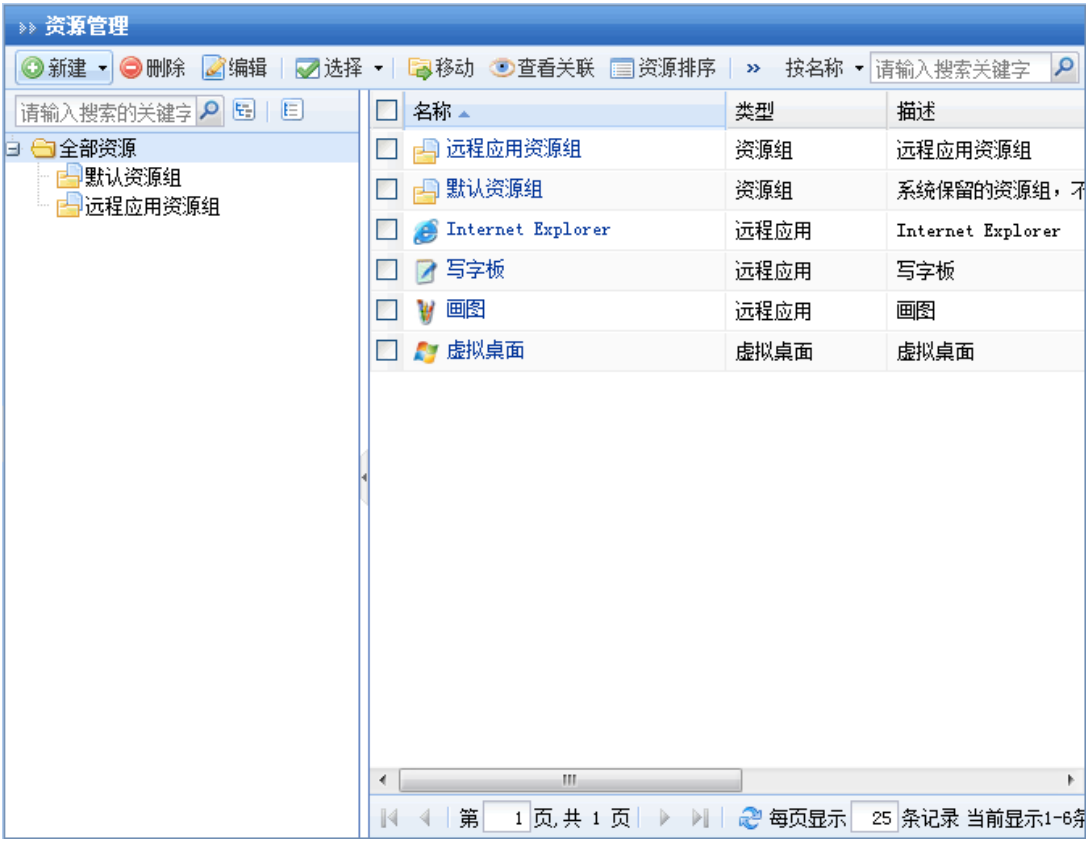
勾选[显示所有（包括子组）]，则会把所有用户都显示到当前页面列表中。

4.5. 资源管理

『资源管理』的主要作用是用户定义 VDI 内网的可用资源，包括[WEB 应用]、[TCP 应用]、[L3VPN]和[远程应用]。

WEBUI 路径：『VDI 设置』→『资源管理』。

界面如下图所示：

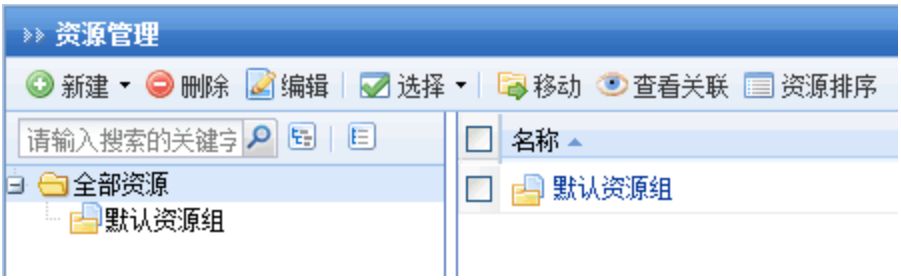


4.5.1. 资源组

为了更好地对资源进行管理、更符合用户使用习惯，以及 VDI 客户端可以更有条理地显示，可以把多个“资源”添加到“资源组”。在资源列表，点击不同的“资源组”显示出该资源组对应“资源”。

WEBUI 路径：『VDI 设置』→『资源管理』→『新建』→『资源组』。

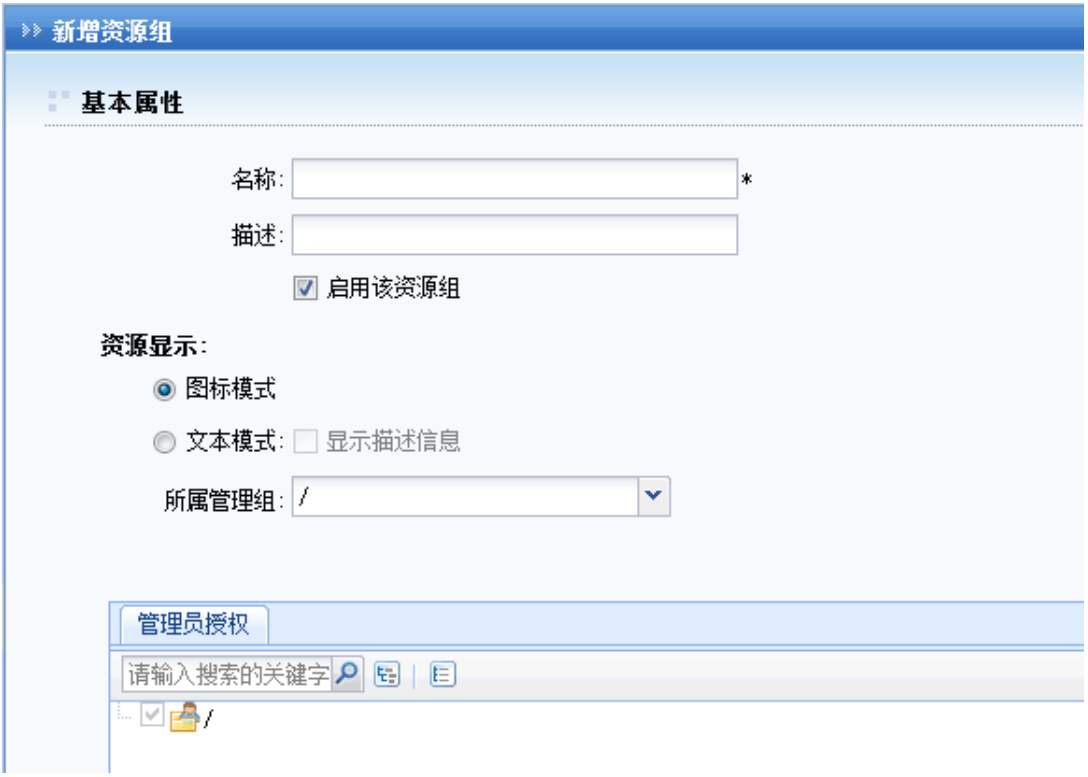
系统默认存在一个资源组，即『默认资源组』，界面如下图所示：



『默认资源组』系统默认保留的资源组，只能够修改，不允许删除。

点击新建按钮，选择[资源组]，如下图：

即弹出【新增资源组】对话框，界面如下图所示：



『名称』和『描述』可随意填写便于理解记忆的文字，在『名称』中填写的文字会显示在 VDI 用户成功登录后，出现的“资源组列表”中。

同一个资源组内的资源在“资源组列表”能够以“图标”或“文本”两种方式显示。

选择[文本显示]，可勾选右边的[显示描述信息]，在“资源组列表”中显示出该“资源组”内“资源”的描述信息。最后点击保存（资源图标的具体设置可参考“资源管理”和“图标管理”章节）。

『所属管理组』即该“资源组”能被哪些管理员编辑和使用。

『管理员授权』在这里可以将下级管理员所创建的资源组的拥有权指派给创建该资源组的上级管理员，原来的管理员将无法编辑自己创建的资源组及该资源组里面的资源。

将下级管理员所创建的资源组的拥有权指派给创建该资源组的上级管理员后，创建该资源的管理员登录控制台后，将无法在资源组和资源页面看见相应的资源组和资源。

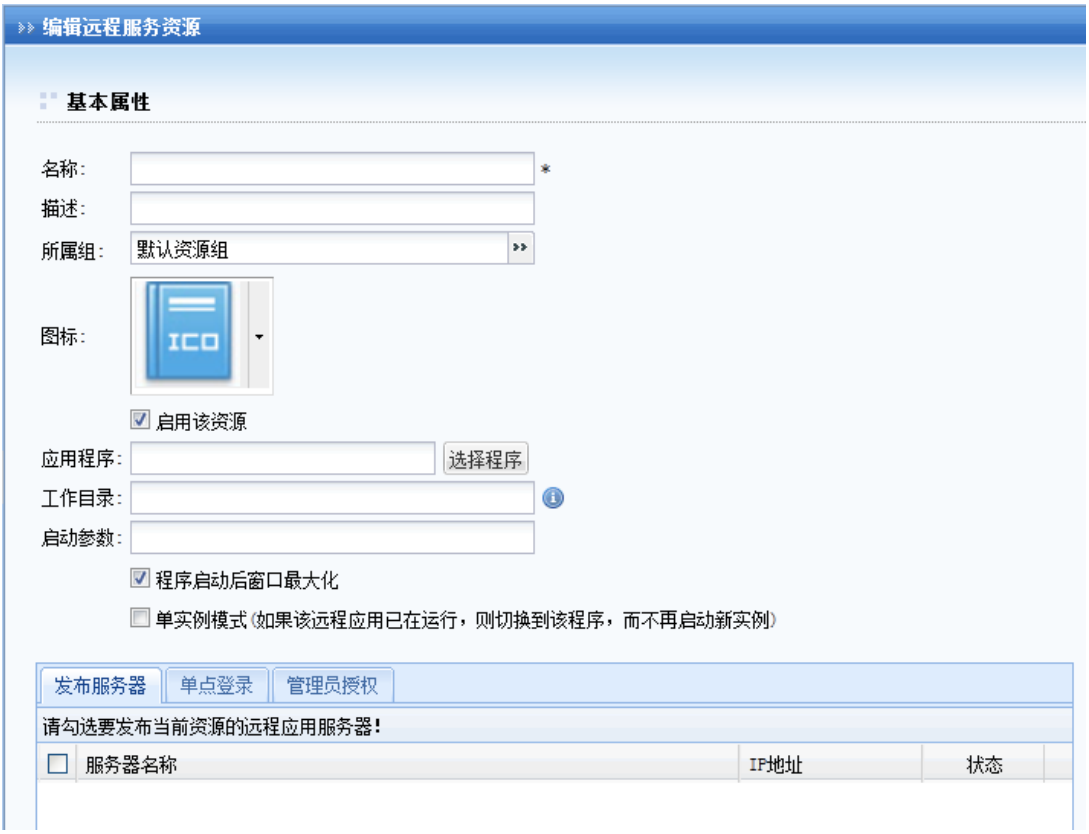
一个“资源”只能够属于一个“资源组”。最多可建立 100 个“资源组”。

4.5.2. 远程应用

『远程应用』主要用于定义、配置和管理各种基于资源服务器的 VDI 内网资源，通过 VDI 来使用内网各种各样的应用程序。

在『资源管理』页面，点击新建按钮，如下图：

选择[远程应用]，弹出【编辑远程服务资源】对话框，设置界面如下：



『名称』和『描述』可随意填写便于理解记忆的文字，『名称』填写的文字会显示在 VDI 用户成功登录 VDI 后，出现的“资源列表”中。

『所属组』可以将该资源划入相应的“资源组”，默认属于“默认资源组”（资源组的具体设置可参考 4.5.1“资源组”章节）。

『图标』，该资源在资源列标中显示的图标。

『应用程序』选择终端服务器提供的应用，点击后面的选择程序，可以选择已添加好的终端服务器提供服务的应用程序，如下图：

添加终端服务器可以参考 4.3“服务器设置”章节。

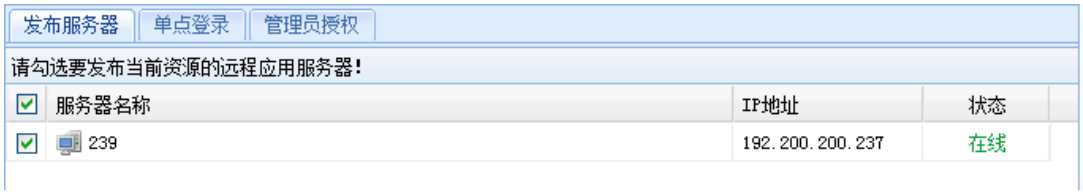
『工作目录』该应用程序在终端服务器的路径。

『启动参数』用来设置程序启用时可能用到的参数。

[程序启动后窗口最大化]，勾选上后远程应用发布的程序启动后，窗口直接就最大化。

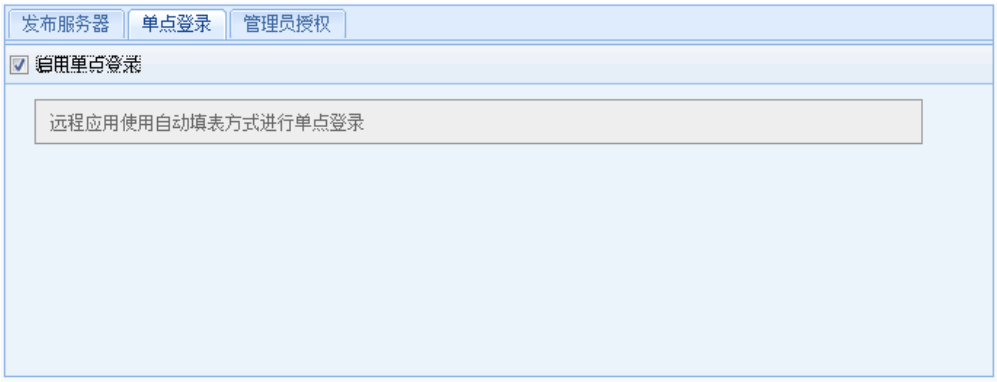
[单实例模式]勾选上后，如果该用户已经启动了一个远程发布资源，再次点击资源的时候不会重新打开，会直接跳到之前打开的资源窗口上。若该资源关联了不同的启动参数，则不建议使用此选项。

『发布服务器』选择需要发布的终端服务器，配置界面如下图：



勾选服务器名称，并保存配置即可。

『单点登录』用于启用远程应用资源的单点登录。如果勾选[启用单点登录]，同时管理员录制了单点登录信息，那么用户登录 VPN 后，访问相应的远程应用资源，则完成相应的单点登录过程。如下图：

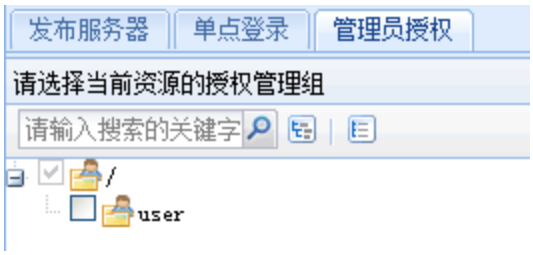


1.远程应用资源单点登录，仅支持自动填表的方式。

2.远程应用单点登录资源，若应用程序选择发布“浏览器”，仅支持发布 IE 内核的浏览器。

3.录制远程应用资源单点登录时，仅 “IE”当做BS资源，其它均为CS资源。

『管理员授权』可将该资源指派给其他管理员，使其他管理员对该资源拥有使用和指派的权限。



资源指派给管理员后，这部分管理员只具备对该资源的使用权、指派给该管理员的下属管理员的权限，对该资源不具备编辑权，用这部分管理员帐号登录控制台后，只能在角色管理中给用户或者用户组关联指派的资源，无法在资源管理中看见这些资

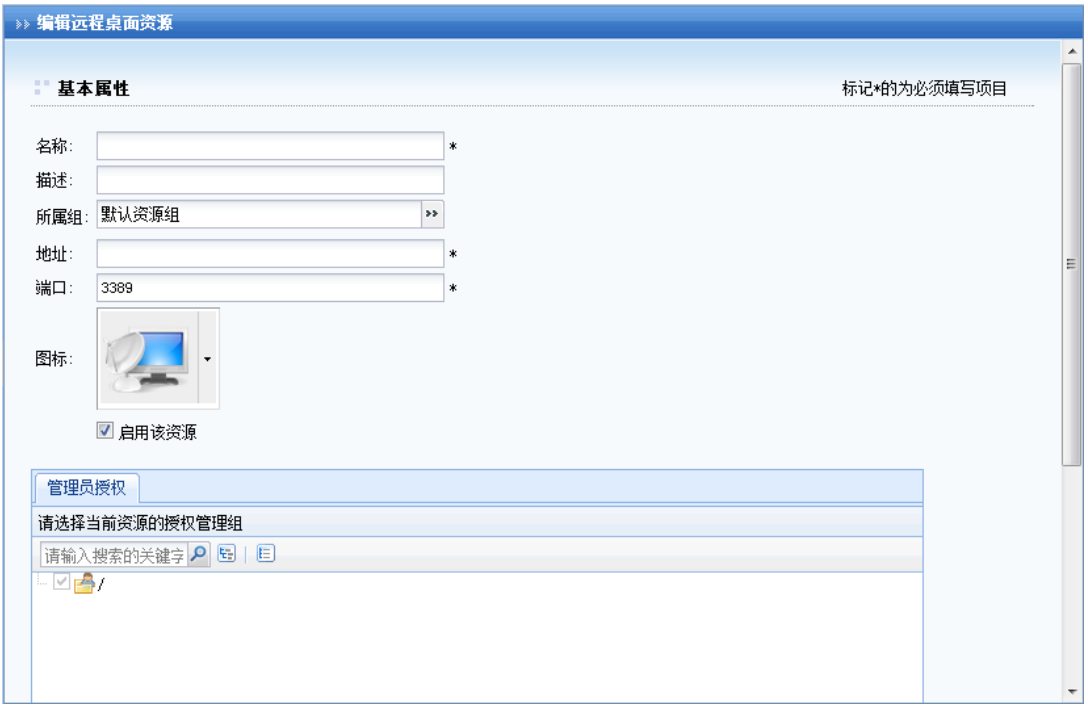
源列表。编辑权仅属于创建该资源的管理员或其上级管理员。

4.5.3. 远程桌面

『桌面』主要用于定义、配置和管理远程桌面资源。

在『资源管理』页面，点击新建按钮，如下图：

选择[远程桌面]，弹出【编辑远程桌面资源】对话框，设置界面如下：



『名称』和『描述』可随意填写便于理解记忆的文字，『名称』填写的文字会显示在 VDI 用户成功登录 VDI 后，出现的“资源列表”中。

『所属组』可以将该资源划入相应的“资源组”，默认属于“默认资源组”（资源组的具体设置可参考 4.5.1“资源组”章节）。

地址：远程桌面服务器的地址。

端口：远程桌面端口，默认为 3389.

『图标』该资源在资源列标中显示的图标。

『管理员授权』可将该资源指派给其他管理员，使其他管理员对该资源拥有使用和指派的权限。

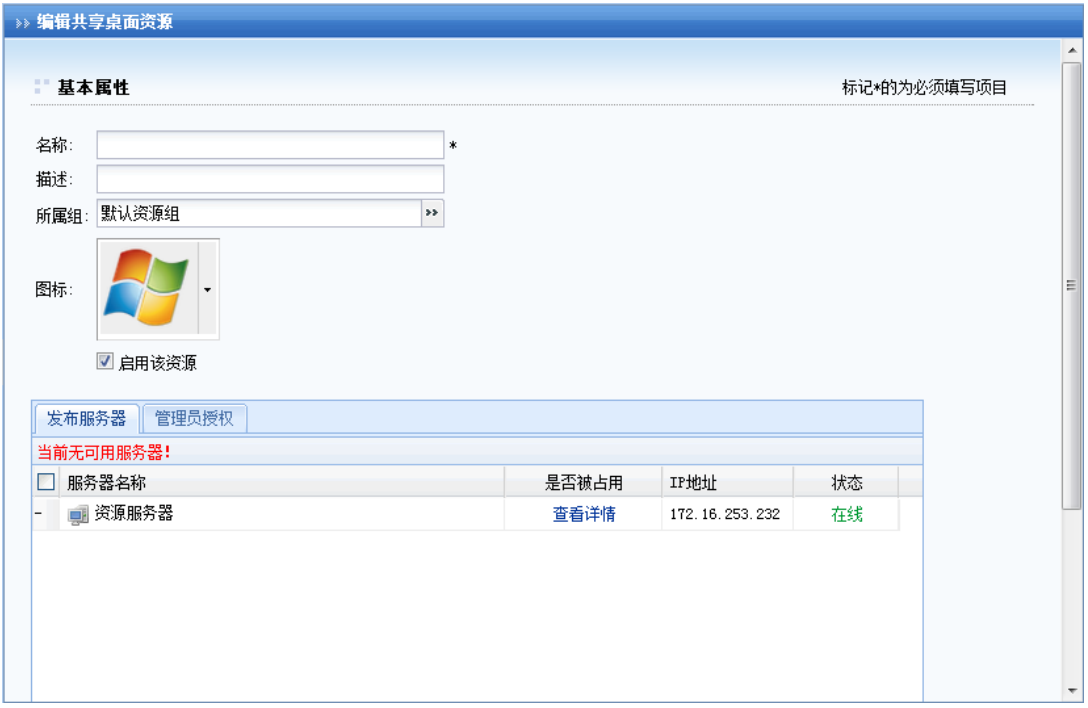
资源指派给管理员后，这部分管理员只具备对该资源的使用权、指派给该管理员的下属管理员的权限，对该资源不具备编辑权，用这部分管理员帐号登录控制台后，只能在角色管理中给用户或者用户组关联指派的资源，无法在资源管理中看见这些资源列表。编辑权仅属于创建该资源的管理员或其上级管理员。

4.5.4. 共享桌面

『共享桌面』主要用于定义、配置和管理共享桌面资源。

在『资源管理』页面，点击新建按钮，如下图：

选择[共享桌面]，弹出【编辑共享桌面资源】对话框，设置界面如下：



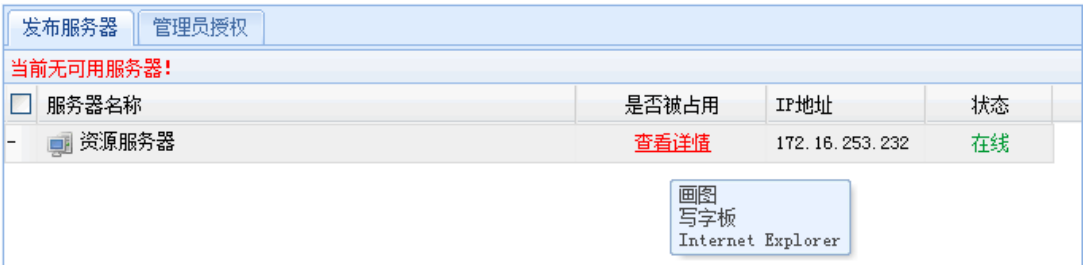
『名称』和『描述』可随意填写便于理解记忆的文字，『名称』填写的文字会显示在 VDI 用户成功登录 VDI 后，出现的“资源列表”中。

『所属组』可以将该资源划入相应的“资源组”，默认属于“默认资源组”（资源组的具体设置可参考 4.5.1“资源组”章节）。

『图标』该资源在资源列标中显示的图标。

『发布服务器』选择用于提供共享桌面服务的服务器。共享桌面服务器与远程应用服务器相同，但是如果服务器已经用于发布远程应用，则不能再用于发布共享桌面。

点击是否被占用一列，可以查看该服务器已发布的远程应用。



『管理员授权』可将该资源指派给其他管理员，使其他管理员对该资源拥有使用和指派的权限。

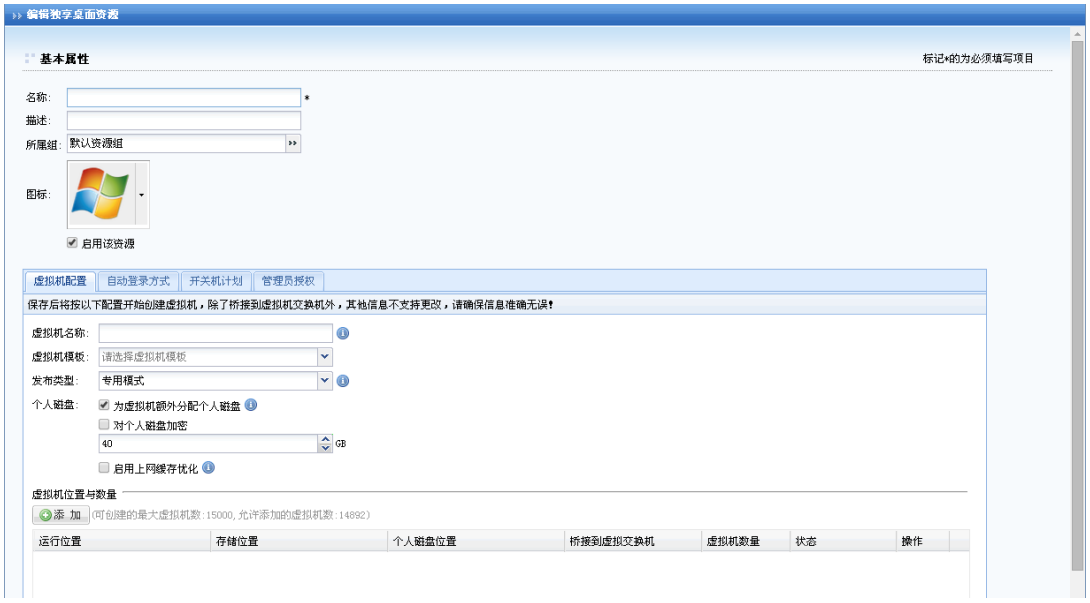
资源指派给管理员后，这部分管理员只具备对该资源的使用权、指派给该管理员的下属管理员的权限，对该资源不具备编辑权，用这部分管理员帐号登录控制台后，只能在角色管理中给用户或者用户组关联指派的资源，无法在资源管理中看见这些资源列表。编辑权仅属于创建该资源的管理员或其上级管理员。

4.5.5. 独享桌面

『独享桌面』主要用于定义、配置和管理远程桌面到虚拟机。

在『资源管理』页面，点击新建按钮，如下图：

选择[独享桌面]，弹出【编辑独享桌面资源】对话框，设置界面如下：



『名称』和『描述』可随意填写便于理解记忆的文字，『名称』填写的文字会显示在用户成功登录后出现的“资源列表”中。

『所属组』可以将该资源划入相应的“资源组”，默认属于“默认资源组”（资源组的具体设置可参考 4.5.1“资源组”章节）。

『图标』该资源在资源列标中显示的图标。

『虚拟机配置』用于配置选择从虚拟化平台控制器中获取已有的虚拟机或重新创建虚拟机以发布到虚拟桌面接入管理系统中。

[虚拟机名称]创建虚拟机的名称模板，用于唯一标识虚拟机。虚拟机的实际名称会自动生成形式如“虚拟机名称-编号”的名称，当相应的虚拟机被绑定给用户后，名称会变为“虚拟机名称-用户名”的格式。

[虚拟机模板]选择虚拟化平台控制器中创建的虚拟机模板，选择后将根据该模板自动派生出虚拟机。

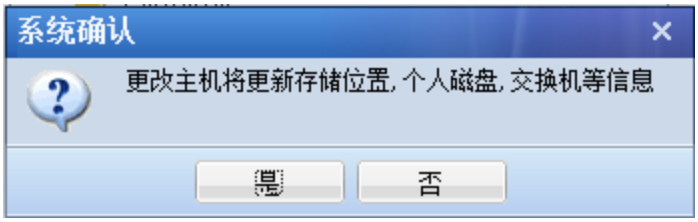
[发布类型]选择虚拟机发布的类型。包括“专用模式”和“还原模式”。“专用模式”即该虚拟机独立给指定的用户使用，用户在虚拟机中做到任何修改将会保留，重启不会丢失。“还原模式”会在虚拟机重启后恢复到初始状态，用户做的一些操作会还原，但会保留个人磁盘的数据，包括我的文档和桌面等数据，勾选自动还原桌面选项可以在用户修改桌面内容重启后会自动恢复。

[个人磁盘]为每个虚拟机分配一个独立的磁盘，在还原模式下该磁盘的数据不会在重启后被清空。分配后绑定用户的我的文档等数据会被重定向到个人磁盘中保存。勾选“对个人磁盘加密”，可针对个人磁盘加密。勾选“启用上网缓存优化”，将启用上网优化功能，此功能采用浏览器缓存重定向技术，提升用户上网体验，但此配置必须在虚拟机内存大于 2.5G 才生效，因为需要将 512MB 的内存转化为虚拟磁盘。

点击添加以添加虚拟机。

[运行位置]选择虚拟机将在哪台主机或集群上运行，即使用哪台主机的 CPU 和内存等资源。

更改运行的主机，将会更新存储位置、个人磁盘和交换机等信息，提示如下：

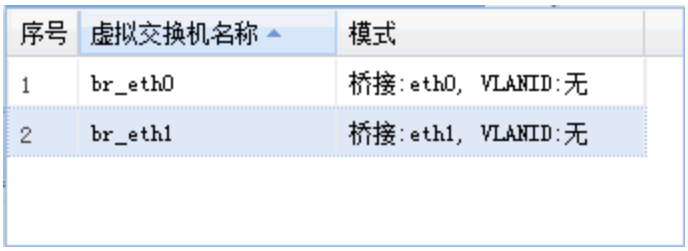


[存储位置]选择派生虚拟机的系统存储位置，即虚拟机系统盘所在的存储位置。如果虚拟机运行位置为某主机，则存储位置可以是该主机的 local 存储或共享存储。如果运行位置为集群，则存储位置只能是共享存储。

序号	存储名称	存储类型	容量	可用空间
1	NFS	nfs	155.51 GB	134.77 GB
2	local	local	892 GB	670.86 GB

[个人磁盘位置] 选择派生虚拟机的个人存储位置，即用户个人数据的存储位置。

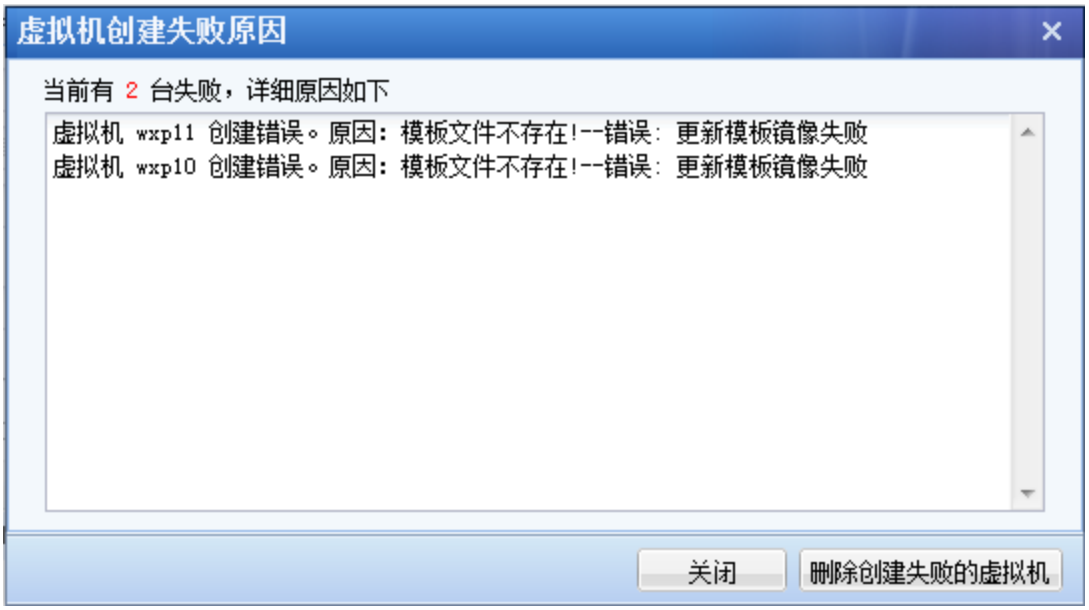
[桥接到虚拟交换机]虚拟机使用的网络接口。如果虚拟机运行位置为某主机，则可以桥接的虚拟交换机只能是该主机上的虚拟交换机。如果运行位置为集群，则桥接的虚拟交换机只能是集群中所有主机上都拥有的相同名称的虚拟交换机。



[虚拟机数量]需要添加的虚拟机数量。

点击确定后，页面将列表显示虚拟机的配置。点击 删除当前配置，点击 编辑该虚拟机配置。如果虚拟机状态为创建成功，则编辑仅限于虚拟交换机和虚拟机数量。

虚拟机创建完成后，会在状态一列显示创建状态。如果创建失败，会在旁边显示原因，点击以查看创建失败原因。



点击删除创建失败的虚拟机，则会将创建失败的虚拟机从虚拟机列表中删除，同时重新计算虚拟机数量。如需重新创建，可以修改虚拟机数量，保存配置后重新创建虚拟机。

『自动登录方式』用于配置用户以什么方式登录到虚拟机。

勾选启动自动登录复选框，可以实现虚拟机自动登陆。

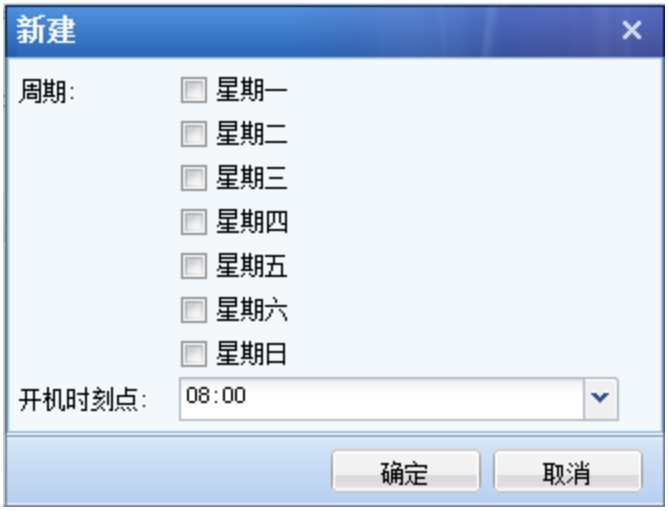
[使用本地帐号自动登录] 如果 VDI 账号未使用密码/证书认证等，则默认使用此处配置的模板系统账号作为本地账号登录。如果 VDI 账号已使用密码认证，则虚拟机操作系统的密码将自动同步为 VDI 账号的密码，以登录 VDI 的帐号登录到虚拟机。

[使用域帐号自动登录] 使用此方式，需要虚拟机加入到域，且以用户账号(VDI 账号)作为域账号登录到虚拟机。勾选此项自动登录方式，需要设置域登录认证以使虚拟机可以加入到域。

『开关机计划』用于配置虚拟机的自动开关机安排。

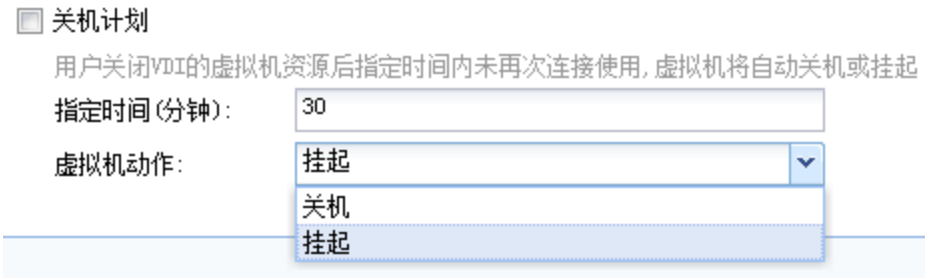
[开机计划]关闭或挂起状态的虚拟机将在下面指定的开机时刻点自动开机。

新建开机时刻点，虚拟机会在设置的时间点自动开机。如图：



勾选不需要的开机时刻点，进行删除操作。

[关机计划] 用户停止使用虚拟机资源后，指定时长内未再次连接使用，虚拟机将自动关机或挂起。



指定时间：设置虚拟机关机或挂起前的超时时间。

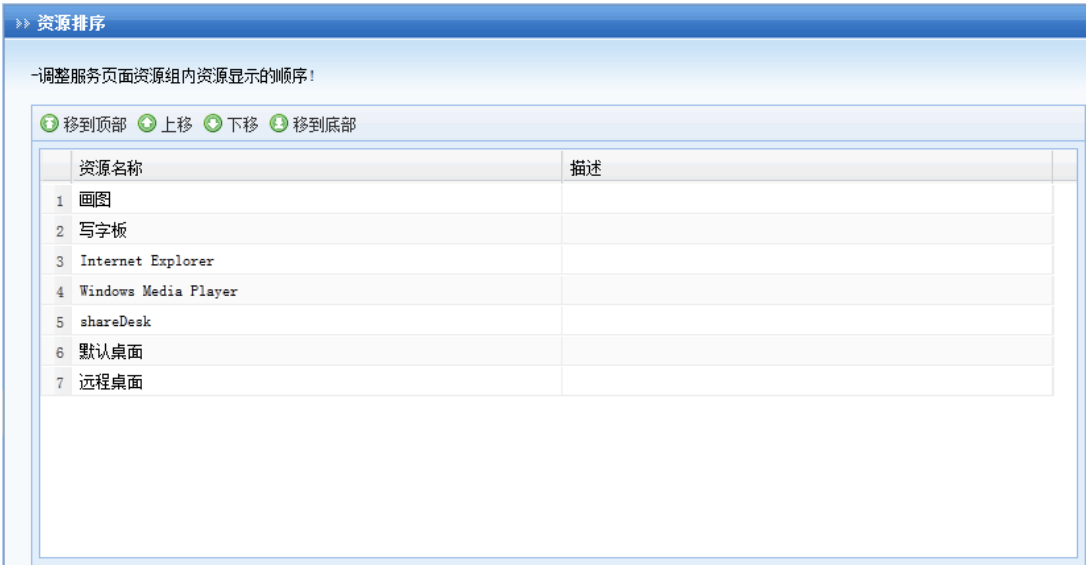
虚拟机动作：设置超时后虚拟机进行关机还是挂起操作。

『管理员授权』可将该资源指派给其他管理员，使其他管理员对该资源拥有使用和指派的权限。

资源指派给管理员后，这部分管理员只具备对该资源的使用权、指派给该管理员的下属管理员的权限，对该资源不具备编辑权，用这部分管理员帐号登录控制台后，只能在角色管理中给用户或者用户组关联指派的资源，无法在资源管理中看见这些资源列表。编辑权仅属于创建该资源的管理员或其上级管理员。

4.5.6. 资源排序

『资源排序』可以对资源组中的各个资源进行排序。可通过上移、下移、移到底部或移到顶部来调整资源顺序。如下图：



除了上述操作外，在资源管理页面，还可对资源进行删除、编辑、移动、筛选等操作：

勾选相应的资源，点击删除，即可删除该资源。

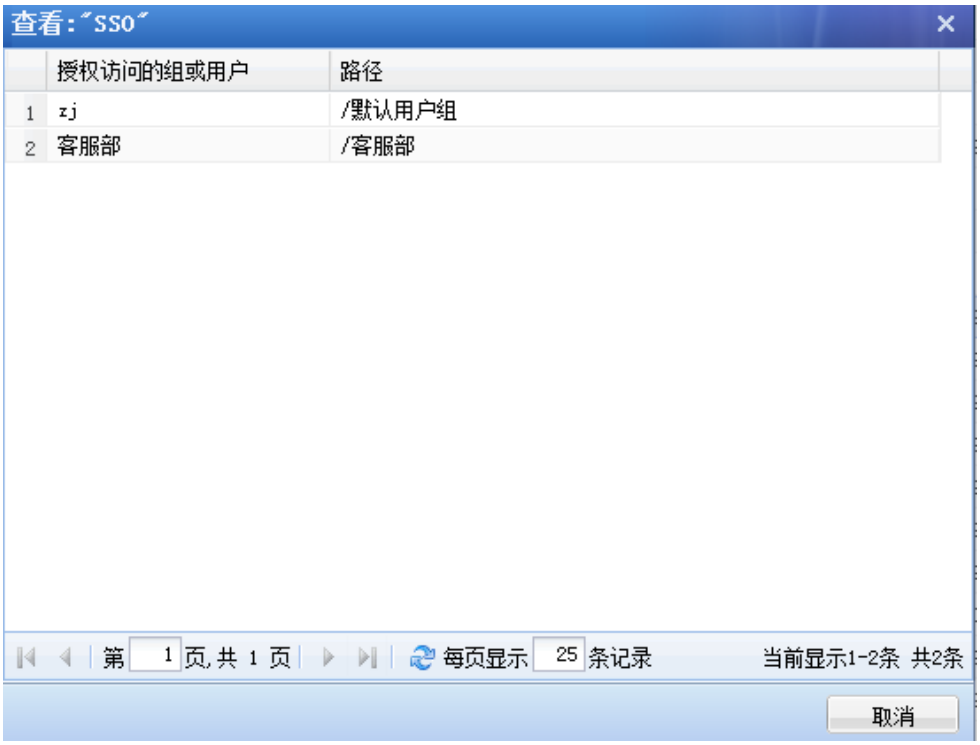
勾选相应的资源，点击编辑，可以该资源进行编辑。

点击选择，可选择当前页或选择所有页的资源，若之前已经选择了资源，也可以取消选择。如下图：

勾选相应的资源，点击移动，可将选中的资源移动到其它资源组中。

注：移动的时候，只能移动资源，不能移动资源组。

勾选相应的资源，点击查看关联，可以查看该资源被哪些用户关联，如下图：



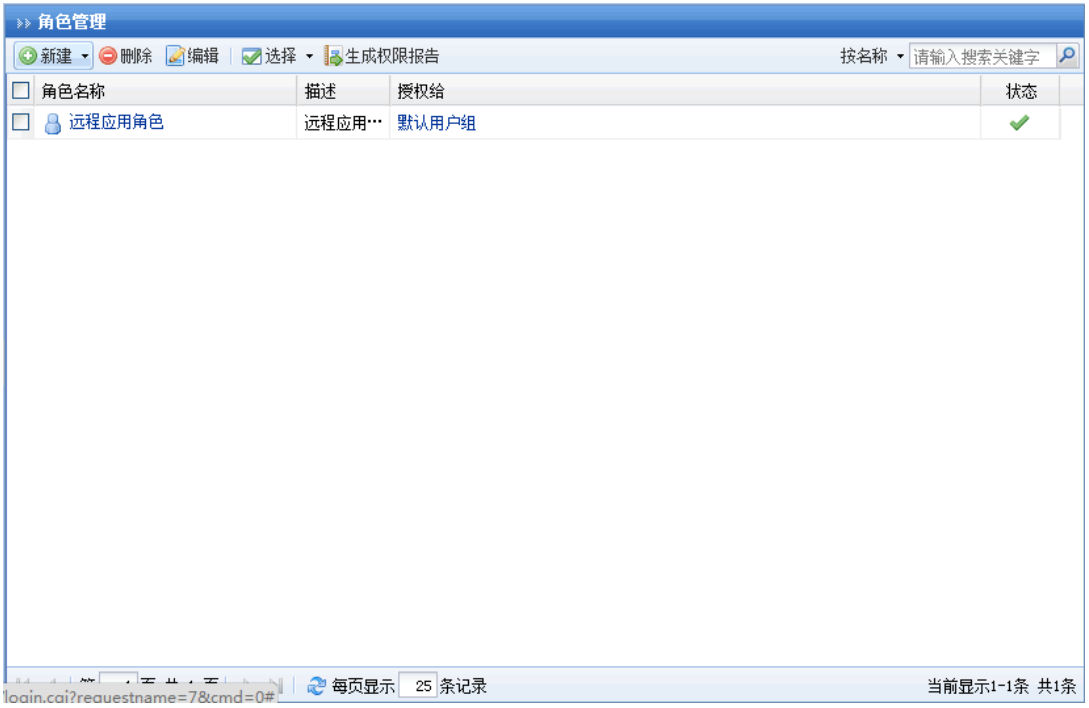
4.6. 角色授权

4.6.1. 新建角色

『角色授权』是“用户/用户组”和“资源”的中介，SANGFOR VDC 正是通过『角色授权』把 VDI 登录用户/用户组和 VDI 资源“关联”起来的。通过角色可以把多个“用户/用户组”、多个资源进行关联，更加有效管理资源和用户组的权限。

WEBUI 路径：『VDI 设置』→『角色授权』。

操作界面如下图所示：



在右上角的输入框内填上需要搜索的目标角色的部分名字，点击  即可筛选出符合条件角色，可以按名称、按描述、按关联的用户（组）来查找角色。

『角色名称』显示角色的名称。

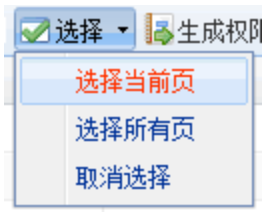
『描述』用来显示角色的描述信息。

『授权给』显示关联了该角色的用户。

点击编辑，用来编辑勾选的角色。

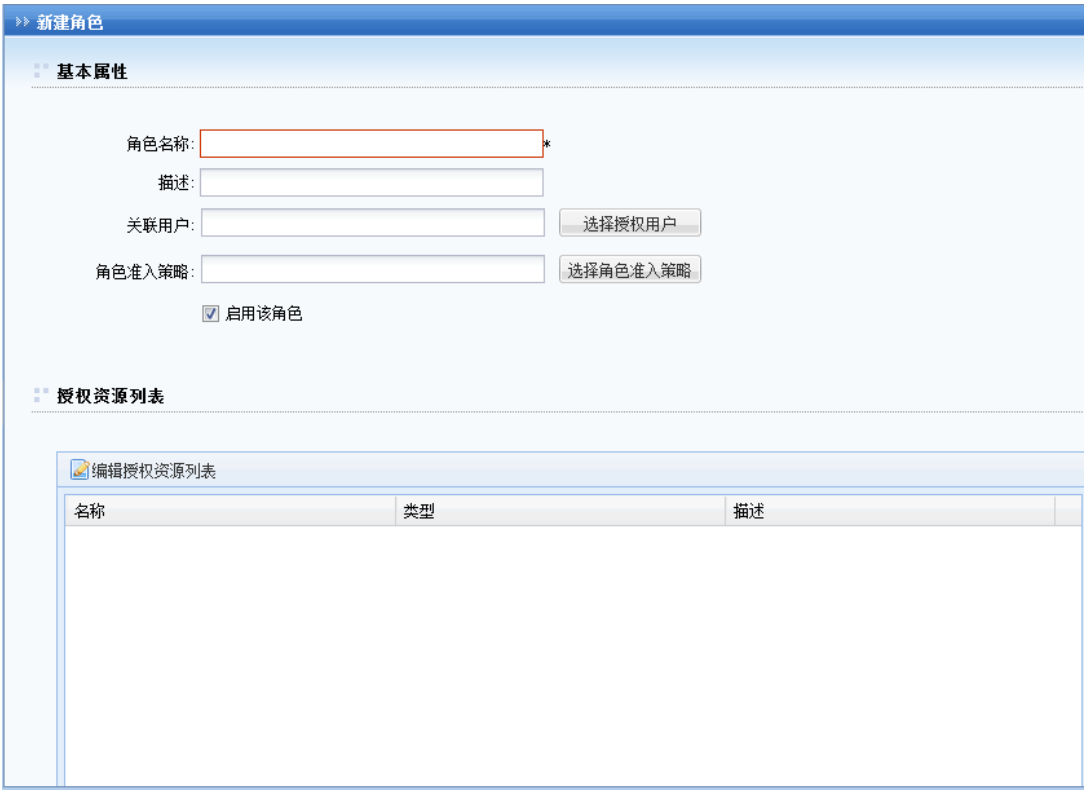
点击删除，用来删除勾选的角色。

点击选择，可以选择当前页或选择所有页。



在角色管理页面，点击新建，可新建角色，如下图：

选择[新建角色]，弹出【新建角色】编辑页面，如下图：



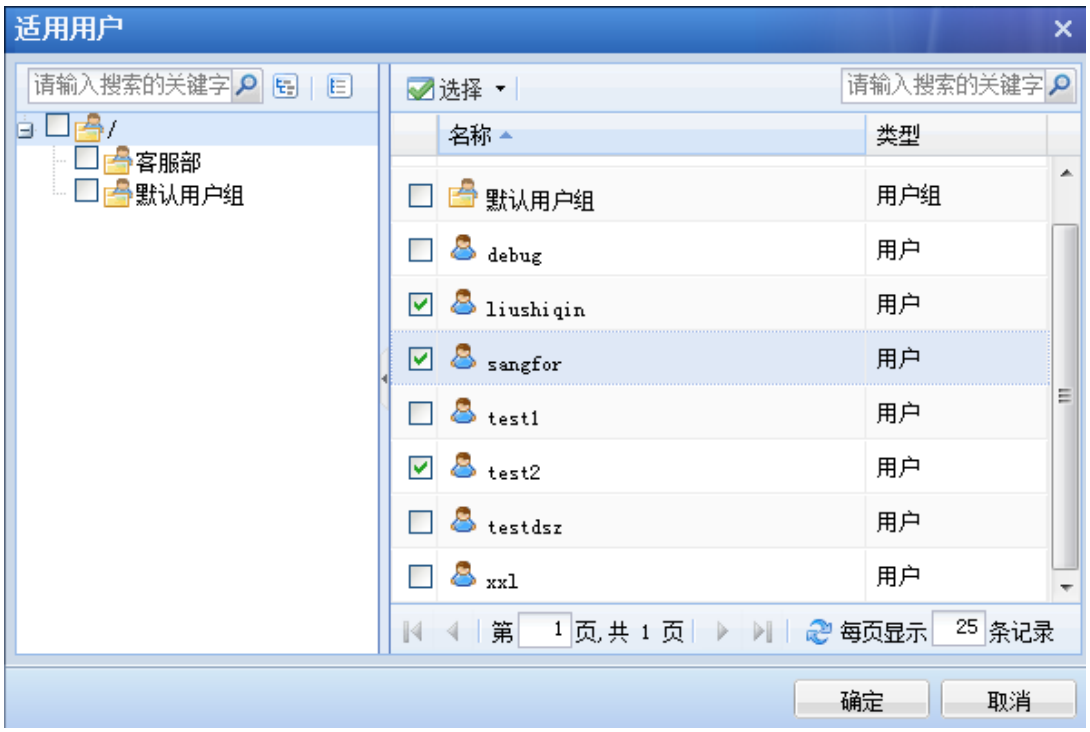
『角色名称』该条角色的名称，自定义即可。

『描述』可随意填写便于理解和记忆的描述语言。

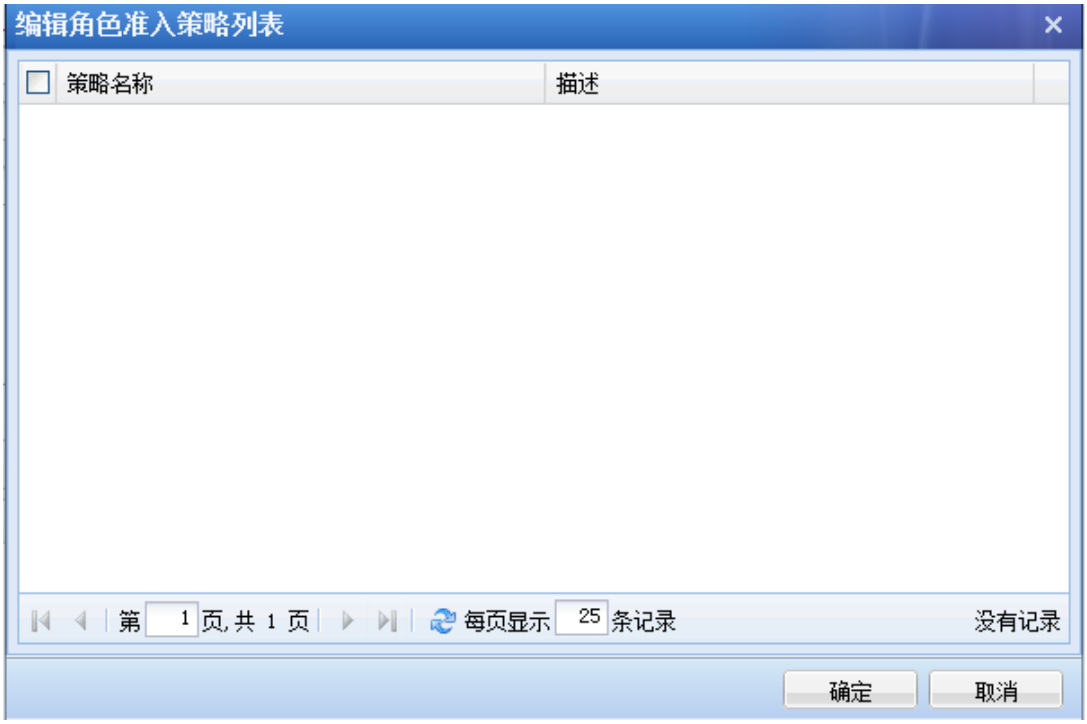
『关联用户』选择关联该条角色的用户或者用户组。

点击选择授权用户按钮，下面的列表会列出『用户管理』中所定义好的用户/组（定义用户/组，请参考 4.4 章节），在列表中勾选相应的用户/组，即可完成“用户/组的关联”，属于该角色的用户，会具有访问该角色关联资源的权限。

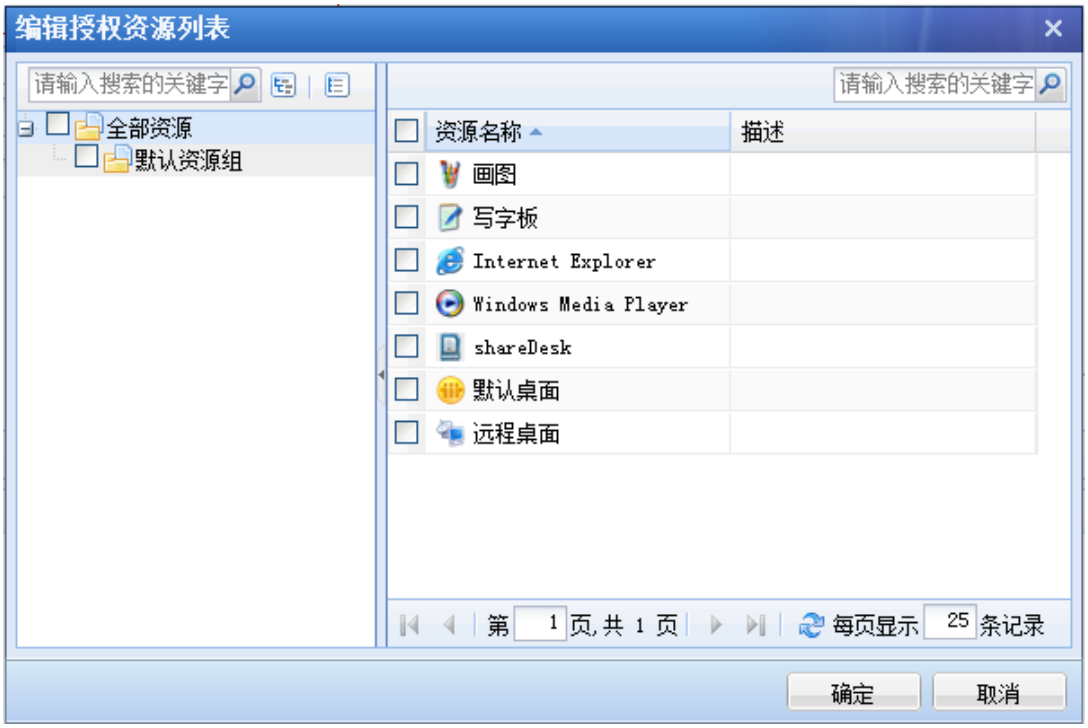
界面如下图所示：



『角色准入策略』，选择该条角色的准入策略，点击选择角色准入策略，弹出【编辑角色准入策略列表】编辑页面（需要先在准入策略设置中添加好相应的策略后这里才可以选择，准入策略设置请参考 4.9.2 章节）勾选相应的策略即可。若没有准入策略，此处可不配置。



在『授权资源列表』设置中，可以设置该角色需要关联的资源。点击编辑授权资源列表按钮，弹出【编辑授权资源列表】页面，选择相应的资源。（资源添加请参考 4.5 章节）界面如下图所示：



选择策略，然后点击确定按钮。确定保存。

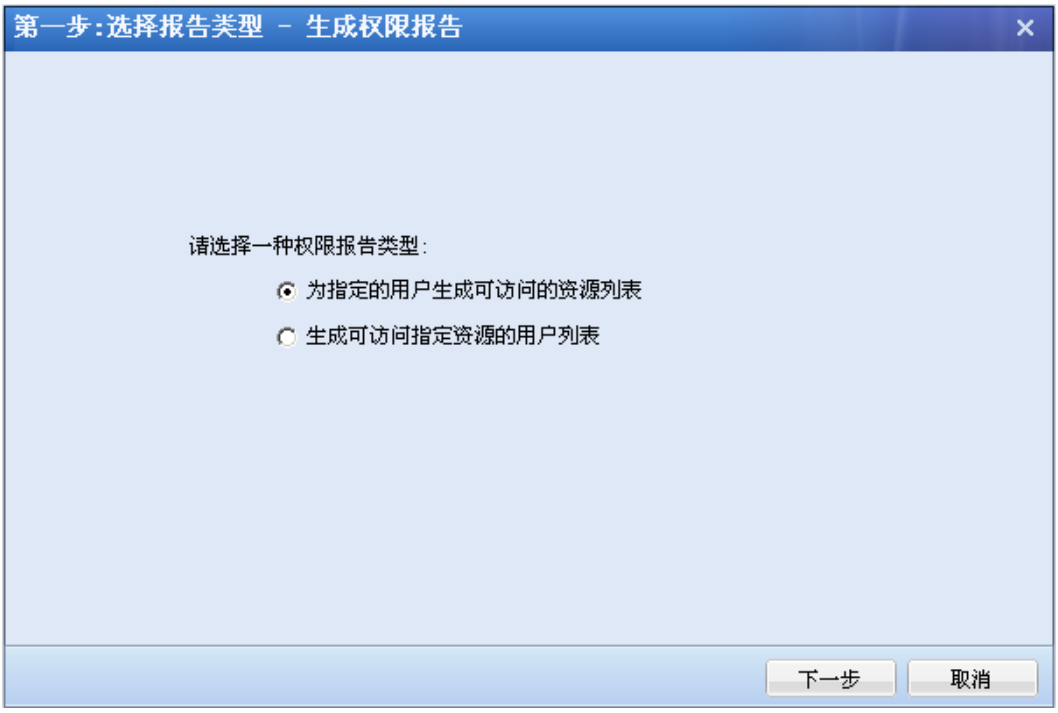
配置完以后，界面如下：

最后点击保存并立即生效，即完成一条角色配置。

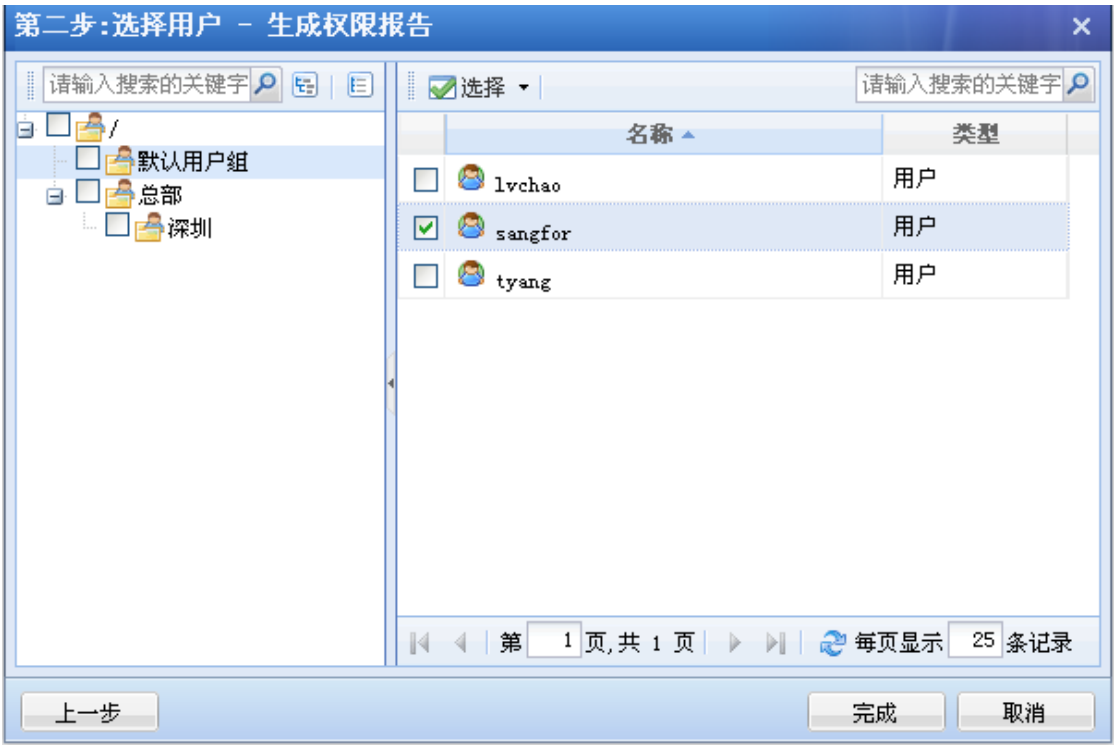
4.6.2. 生成权限报告

『生成权限报告』用来生成显示用户可访问资源的报表。

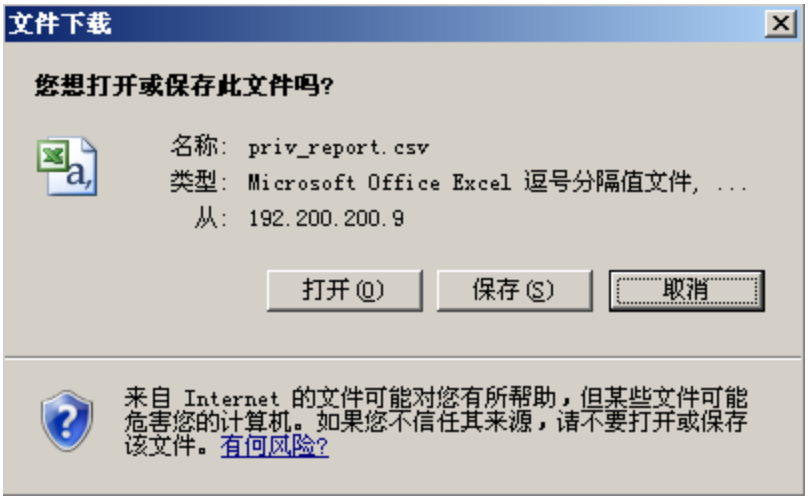
如下图所示：



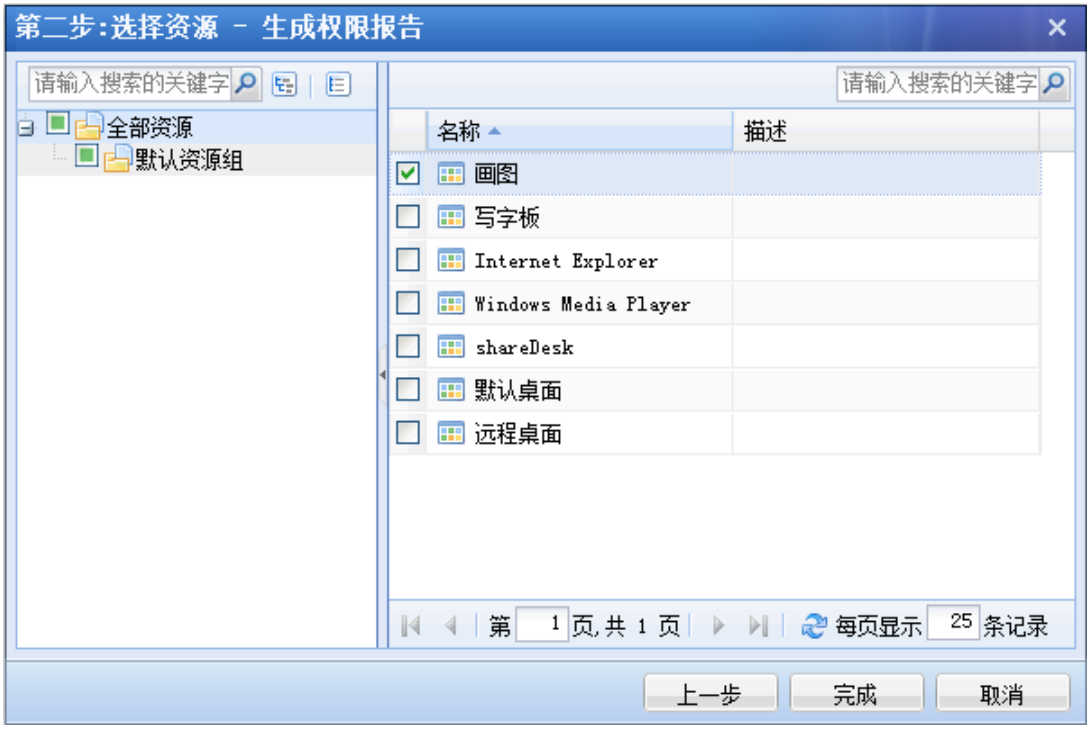
勾选[为指定的用户生成可访问的资源列表]，点击下一步按钮，如下图所示：



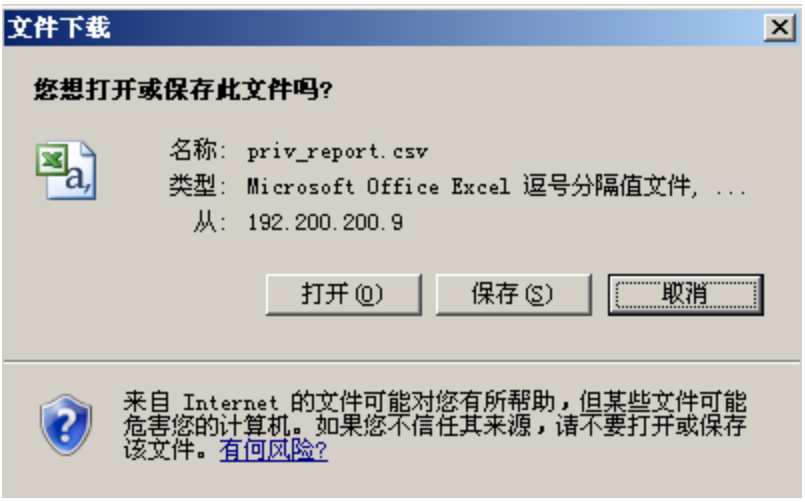
选择用户，点击完成，生成“.csv”格式的文件，如下图所示：



勾选[生成可访问指定资源的用户列表]，点击下一步按钮，如下图所示：



选择资源，点击完成，生成“.csv”格式的文件，如下图所示：



4.7. 认证设置

『认证设置』包含『主要认证』、『辅助认证』和『认证选项设置』。『认证设置』主要用于配置认证服务器，以及各种认证的相关选项。

WEBUI 路径：『控制台』→『VDI 设置』→『认证设置』。

界面如下图所示：

4.7.1. 主要认证

『主要认证』包含『本地密码认证』、『LDAP 认证』、『Radius 认证』、『证书与 USB-KEY 认证』和『域单点登录认证』。

4.7.1.1. 本地密码认证

『本地密码认证』设置页面包含『密码安全策略』、『用户名策略』。

WEBUI 路径：『VDI 设置』→『认证设置』→『主要认证』→『本地密码认证』。页面如下：

点击本地密码认证后面的设置，弹出【本地密码认证设置】页面，界面如下图所示：

『密码安全策略』用于设置用户的一些密码策略，详细可参见上图。

『用户名策略』用户登录时，设置是否区分输入用户名的大小写。

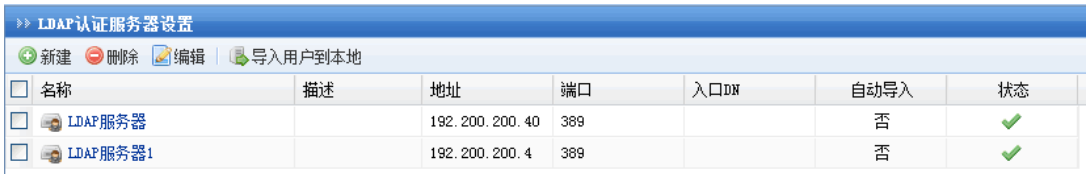
注意：上述策略只对本地密码认证的用户有效。

4.7.1.2. LDAP 认证

SANGFOR VDC 网关支持使用“LDAP 协议”的第三方的服务器作为认证服务器。『LDAP 认证』就是用于设置 LDAP 外部认证服务器相应参数的。

WEBUI 路径：『VDI 设置』→『认证设置』→『主要认证』→『LDAP 认证』。页面如下：

点击 LDAP 认证后面的设置，弹出【LDAP 认证服务器设置】页面，界面如下图所示：



点击新建可新增一个 LDAP 服务器，弹出 LDAP 外部认证服务器的参数设置界面。配置如下图：

『服务器名称』和『服务器描述』可随便填写便于记忆的文字。

『服务器地址』用于设置 LDAP 服务器的 IP 地址和所使用的端口，此处可设置多个

服务器地址和端口，他们之间是主备关系，第一个服务器为主服务器，其余都为备服务器，当第一个服务器连不上，才尝试连接第二个服务器认证，以此类推。

点击图标，出现服务器 IP 地址和端口的设置页面如下：

点击，可以删除所选的服务器地址。

点击，可以编辑所选的服务器地址。

点击或，可以调整服务器地址的顺序。

『管理员全路径（DN）』和『管理员密码』填写 LDAP 服务器内一个有效的账号和密码，用于读取 LDAP 结构。所填写的帐号一般要以域中 DN 的形式填写。

该账号在 LDAP 服务器必须有读取用户路径的权限。

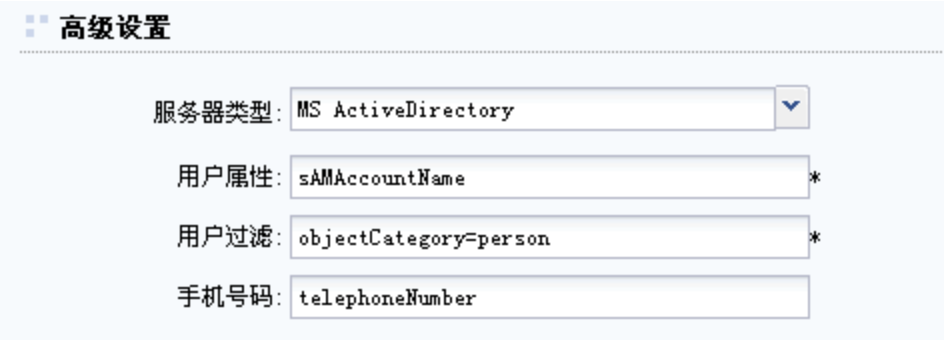
『搜索入口』用于选择需要用于认证的 LDAP 用户账号所在路径。

在所选择用户账号所在路径时，在包含（嵌套）子路径的情况下，若勾选[搜索子树]，该路径下的所有子路径的用户账号都包含进来；若不勾选[搜索子树]，则只包含该路径下的本级用户账号。

『认证超时』当连接到服务器但服务器超过这里所设置的时间仍然没有回应，就认为客户端认证失败。

『是否启用』用于设置是否启用该 LDAP 外部认证服务器。

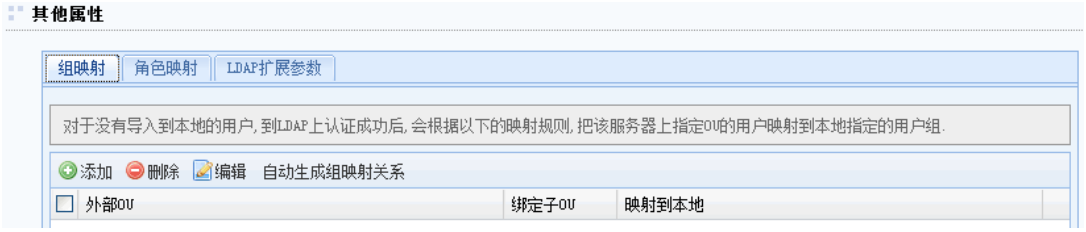
『高级设置』配置如下图：



『高级设置』相关配置，请征询 LDAP 服务器管理员的意见才能进行修改。

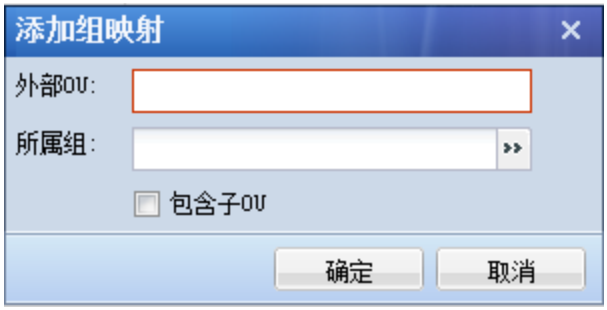
系统支持普通的 LDAP 协议和支持微软的 MS Active Directory 协议。对于 MS-AD，用户是以属性 sAMAccountName 认证属性，以“objectCategory=person”作为过滤用户账号的条件；对于普通 LDAP 协议，用户是以属性 uid 为认证属性，以“objectclass=person”作为过滤用户账号的条件。用户也可以自定义其他属性来得到用户名和组名称。

『其他属性』包含『组映射』、『角色映射』、『LDAP 扩展参数』。如下图：



『组映射』针对没有导入到本地的 LDAP 服务器的用户，用于设置将 LDAP 服务器中的 OU 和 VDC 网关本地的用户组绑定起来，那么该 OU 中的用户登录 VDI 之后就会拥有本地被绑定用户组的权限。配置页面如下图：

点击添加，出现组映射配置页面如下。



『外部 OU』填写需要映射的 OU 在域中的 DN。

『所属组』选择该 OU 所要映射的本地用户组。

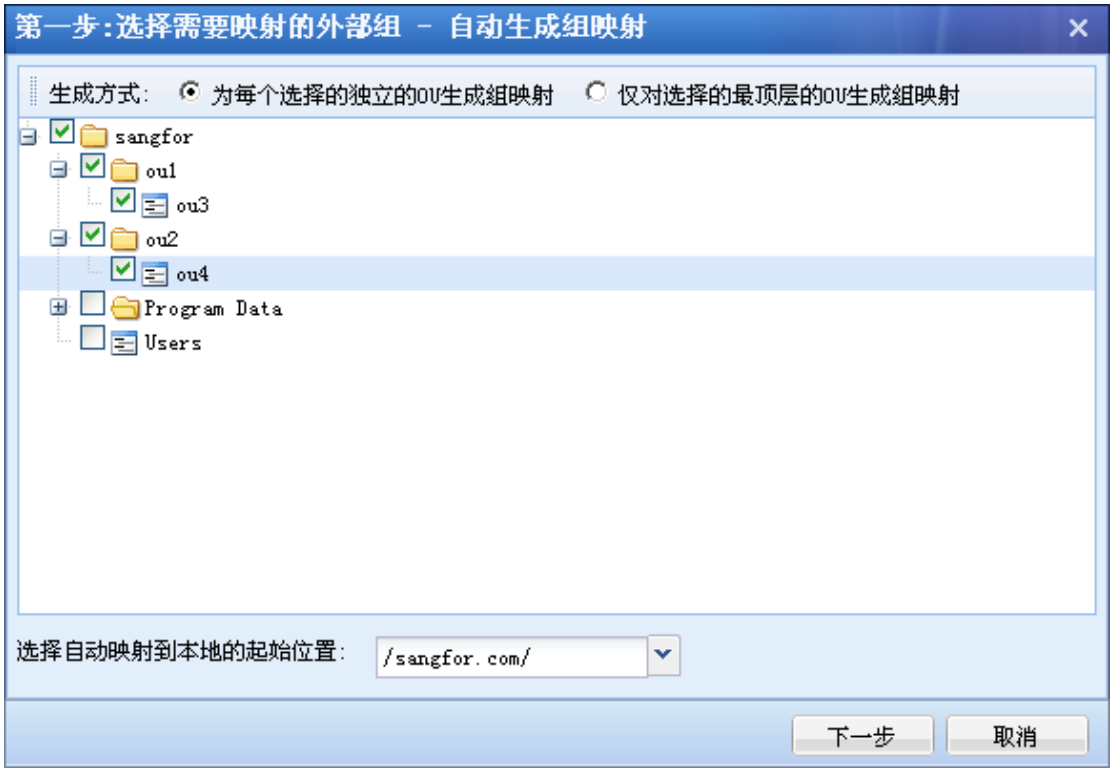
[包含子 OU]用于设置是否包含所选 OU 的子 OU。若勾选[包含子 OU]，则该 OU 下的所有子 OU 的用户账号都包含进来；若不勾选[包含子 OU]，则只包含该 OU 下的本级用户账号。

[如果未设置映射，将其自动映射到目标]用于设置当某个 OU 没有映射到本地用户组的时候，这个 OU 里边的用户认证通过之后自动匹配为那个用户组的用户。

点击删除，可以删除所选的组映射规则。

点击编辑，可以编辑所选的组映射规则。

点击自动生成组映射关系，出现配置页面如下：

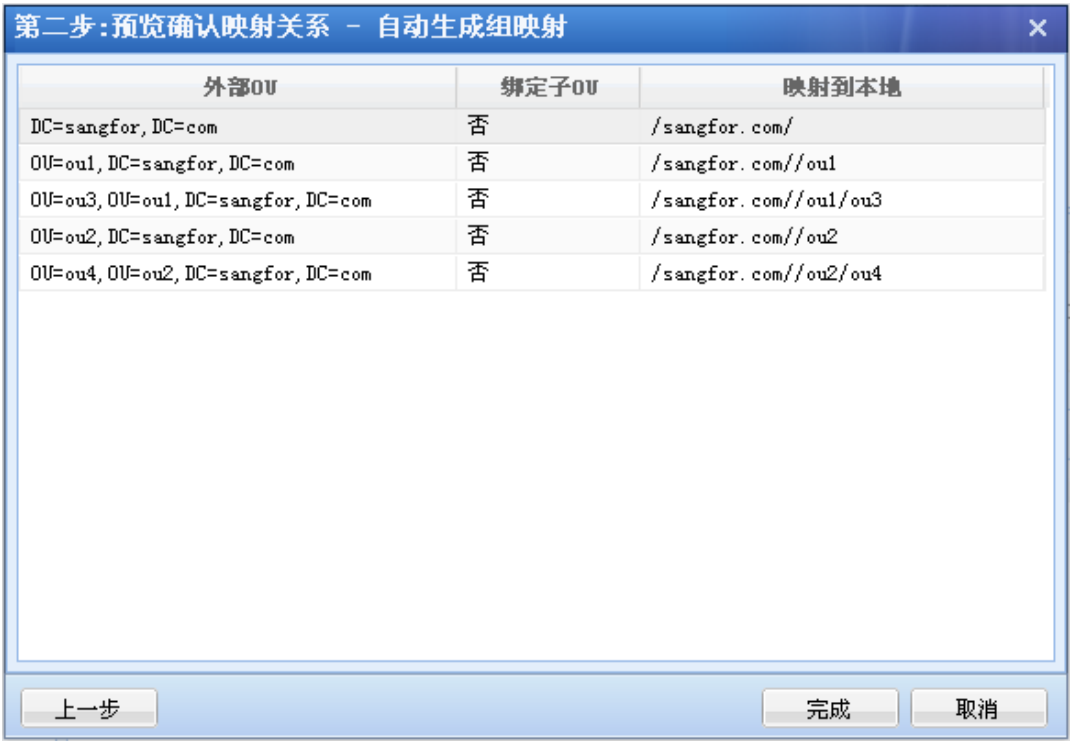


[为每个选择的独立的 OU 生成组映射]用于设置将我们所勾选的所有 OU 都在本地生成一个用户组并自动映射到该组。并且导入之后组织结构不会变化。

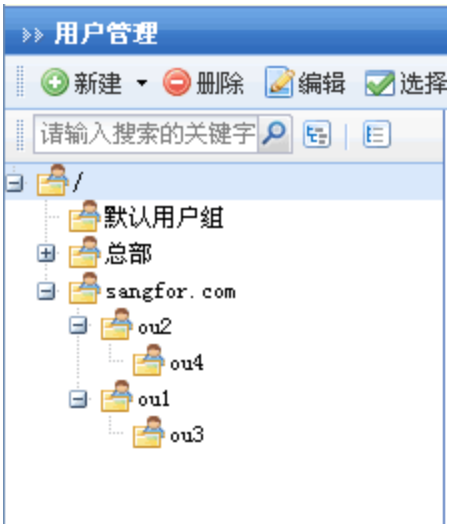
[仅对选择的最顶层的 OU 生成组映射]用于设置只将我们勾选的最上级 OU 在本地生成一个用户组，该 OU 及其下级 OU 都映射到该组。

『选择自动映射到本地的起始位置』用于设置最上级 OU 映射到的本地用户组。

点击下一步，出现预览映射关系页面如下图：



点击完成，则在『用户管理』中生成用户组并一一映射，如下图所示：



『角色映射』用于将 LDAP 服务器中的安全组映射到 VDC 网关本地的角色，那么当域中隶属于该安全组的用户通过 VDI 认证之后自动匹配到该角色，获得该角色中绑定资源的访问权限。配置页面如下图：

『是否启用角色映射』用于启用和禁用角色映射功能。

点击添加，可以添加角色映射规则，配置页面如下图：

『外部安全组』用于设置需要映射的安全组。

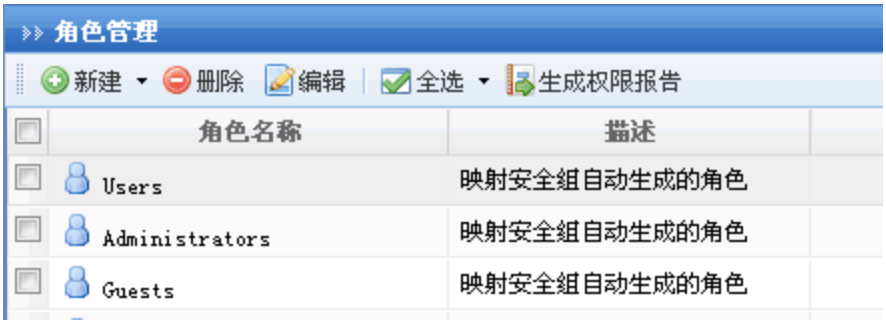
『映射角色』用于设置安全组需要映射到本地的哪个角色。

点击删除，可以删除所选的角色映射规则。

点击编辑，可以编辑所选的角色映射规则。

点击自动生成角色映射关系，出现配置页面如下：

勾选外部安全组，点击确定，则在本地『角色授权』中自动新建同名的角色并映射，如下图所示：



『LDAP 扩展属性』配置页面如下：

[关联资源的属性列表]用于设置当 LDAP 上用户认证成功后，根据关联资源的属性列表配置的信息，给用户分配相关的资源。

点击  ，弹出【添加关联资源属性】，设置需要关联的属性名。配置页面如下：

点击确定，将属性名添加至属性列表中。

点击  ，用于删除选中的属性名。

点击  ，用于编辑选中的属性名。

[继承所有上级资源]用于设置当该 LDAP 服务器上用户登录后，除了所绑定的属性的值作为资源下发到资源列表，该用户所属 OU 以及上级的所有 OU 的该属性的值也会作为资源发到资源列表。

勾选[虚拟 IP 属性名]，在右边方框内填写 LDAP 服务器上作为用户账号 IP 地址的属性名字，该 LDAP 服务器上用户登录后，LDAP 服务器返回该属性值到 VDC 设备，用于该 LDAP 账号下发的虚拟 IP。

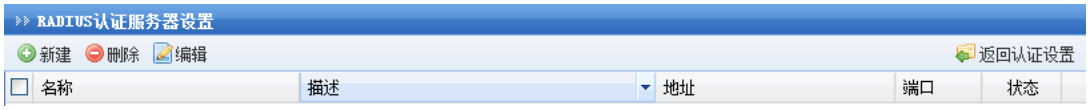
以上『关联资源的属性列表』只对用户列表上不存信息的 LDAP 账号生效，若用户列表存在相应的用户账号，该功能无效。

4.7.1.3. RADIUS 认证

SANGFOR VDC 网关支持使用“RADIUS 协议”的第三方的服务器作为认证服务器。『RADIUS 认证』就是用于设置 RADIUS 外部认证服务器相应参数的。

WEBUI 路径：『VDI 设置』→『认证设置』→『主要认证』→『RADIUS 认证』。页面如下：

点击 Radius 认证后面的设置，弹出【RADIUS 认证服务器设置】页面，如下图：



点击新建出现 RADIUS 外部认证服务器的参数设置界面。参数设置页面包含『基本属性』、『RADIUS 扩展属性』、『组映射』。『基本属性』配置如下图：

『服务器名称』和『服务器描述』可随便填写便于记忆的文字。

『服务器地址』用于设置 RADIUS 服务器的 IP 地址和所使用的端口，此处可设置多个服务器地址和端口，他们之间是主备关系，第一个服务器为主服务器，其余都为备服务器，当第一个服务器连不上，才尝试连接第二个服务器认证，以此类推。

点击  ，出现服务器 IP 地址和端口的设置页面如下：

点击  ，可以删除所选的服务器地址。

点击  ，可以编辑所选的服务器地址。

点击  或  ，可以调整服务器地址的顺序。

『认证协议』可选择为[不加密的协议 PAP]、[咨询握手身份验证协议（CHAP）]、[microsoft CHAP]、[microsoft CHAP 2]或[EAP-MD5]，根据实际情况选择。

『共享密钥』、『字符集』、『认证超时』可根据实际情况填写。

『是否启用』用于设置启用或禁用该外部认证服务器。

『Radius 扩展属性』配置页面如下图：

勾选『绑定手机号码 ID』，在右边第一个方框内填写 RADIUS 服务器上作为用户账号手机号码的属性 ID，第二方框填写子属性 ID。该 RADIUS 服务器上用户登录后，RADIUS 服务器返回该属性值到 VDC 设备，用于短信认证。

注：该功能可与短信认证结合使用。

勾选[绑定虚拟 IP 地址 ID]，在右边第一个方框内填写 RADIUS 服务器上作为用户账号 IP 地址的属性 ID，第二方框填写子属性 ID。该 RADIUS 服务器上用户登录后，RADIUS 服务器返回该属性值到 VDC 设备，用于该 RADIUS 账号使用 L3VPN 时下发的虚拟 IP。

『组映射』用于设置 Radius 的扩展属性值，并映射到本地组，那么当 Radius 认证用户成功认证之后，根据 Radius 中的属性值将用户分配到某个组并拥有访问该组关联资源的权限，配置页面如下图：

点击添加，配置页面如下：

『字段』用于设置 Radius 中的 Class 属性值。

『所属组』用于设置将用户分配到的本地组。

点击确定，将设置的映射规则添加到映射规则列表。

点击删除，删除选中的映射规则。

点击编辑，编辑选中的映射规则。

『如果未设置映射，将其自动映射到目标』用于设置当成功登录 VDI 的用户，找不到对应的组映射规则时，将该用户分配到的本地用户组。

4.7.1.4. 证书与 USB-KEY 认证

SANGFOR VDC 不仅支持同时使用内置 CA 和外部 CA 进行认证，还可支持使用多个外部 CA。对于总部部署了 VDC 设备，各个分支接入用户使用不同的第三方 CA 进行认证的情况，大大的增加了 VDI 部署的灵活性。『证书与 USB-KEY 认证』正是用于生成、配置和管理 CA 的数字证书等方面。

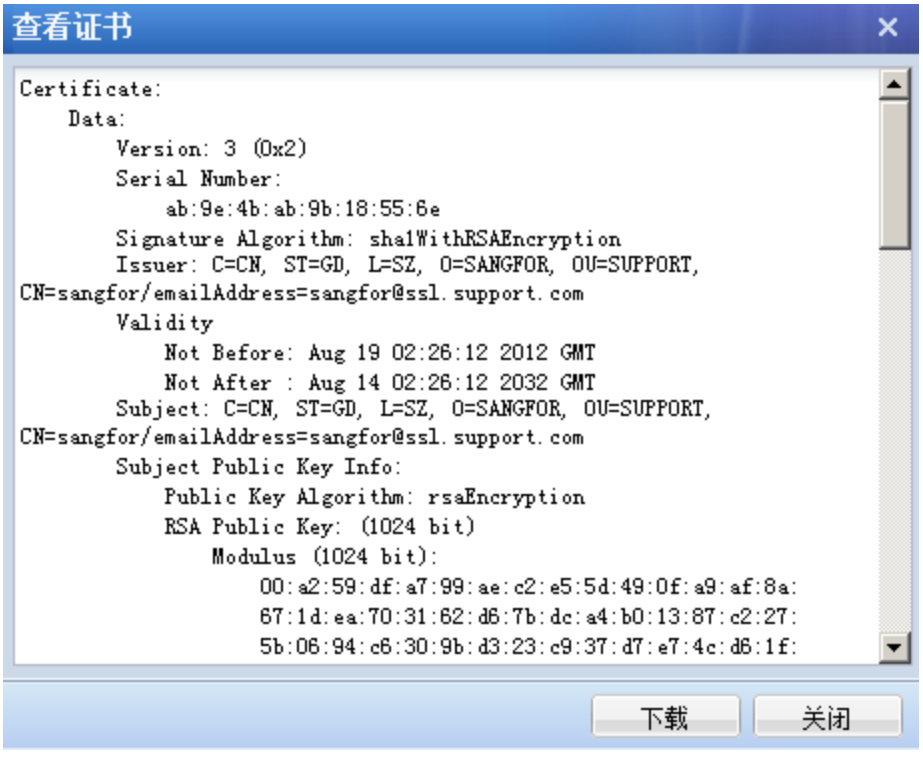
WEBUI 路径：『VDI 设置』→『认证设置』→『主要认证』→『证书与 USB-KEY 认证』。页面如下：

点击下载安装 USB-KEY 驱动，可以手动安装 USB-KEY 驱动程序。

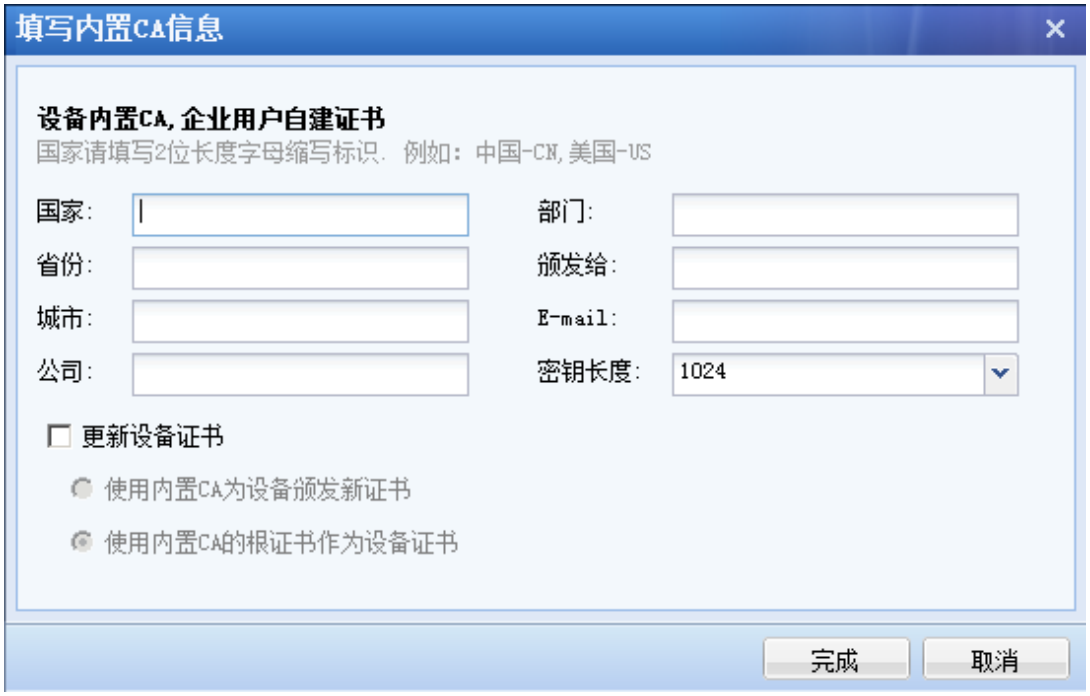
点击下载安装导入控件，可以手动安装证导入证书控件。

点击设置，弹出【证书与 USB-KEY 设置】页面，可启用和禁用内置 CA，配置第三方 CA，查看在线证书和通用 USB 设置等。各部分配置页面如下：

点击内置 CA 的查看按钮，查看内置 CA 的根证书，显示如下：



点击内置 CA 的更新按钮，设置页面如下图：



输入证书所需的各项信息，点击完成生成根证书。

注意：自建 CA 时，国家名为 2 个英文字符。例如：CN。邮件地址不支持中文。

如果勾选了[更新设备证书]，并选择[使用内置 CA 为设备颁发新证书]，点击下一步，则出现内置 SSL 证书信息设置页面，如下图：

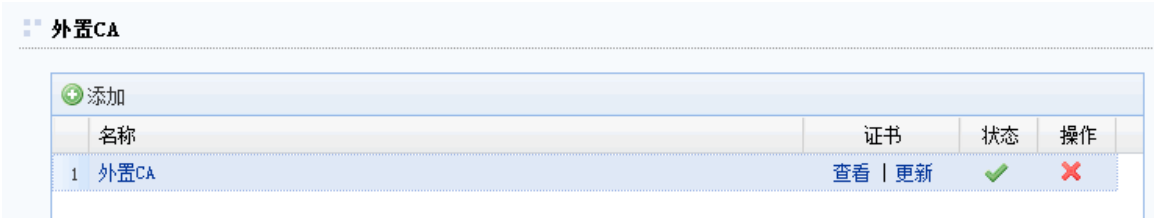
输入证书所需各项信息之后，点击完成，此时根据所填写根证书及 SSL 证书信息同时生成根证书和 SSL 证书；.

如果勾选了[更新设备证书]，并选择[使用内置 CA 的根证书作为设备证书]，点击完成，此时生成根证书并将根证书同时作为设备证书。

点击签发用户证书，生成一个证书，该证书可作为用户证书也可作为服务器证书。

点击外置 CA 的添加按钮，添加外置 CA，同时支持 7 个外置 CA 的认证，显示如下：

导入外置 CA 证书并设置 CA 名称，点击确定保存。添加成功后，显示如下：



点击证书名称，设置证书相关选项。

[用户名属性] 是指此 CA 签发的证书中，存放用户名的字段；用户名将显示在客户端主界面上，支持使用 CN、Email 前缀和 OID 作为用户名属性。

[绑定字段] 指此 CA 颁发的证书导入到本地时，用户所绑定的证书字段。

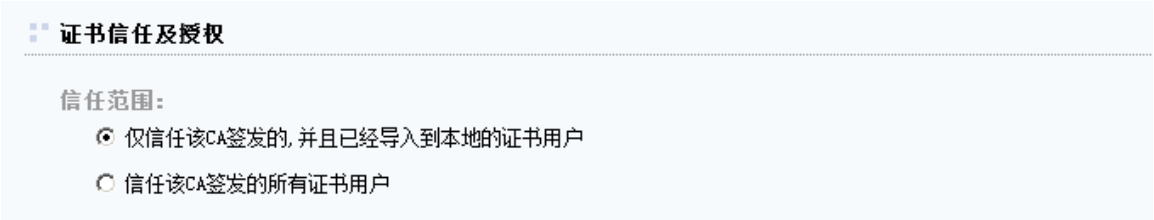
序列号：证书过期后，CA 会重新签发证书，因为新证书的序列号已改变，必须在本

地用户管理中，重新导入新证书；

DN：相比证书序列号，可以避免用户证书更新时需要重新导入证书。选择此选项时，必须保证不同证书的 DN 名是唯一的；

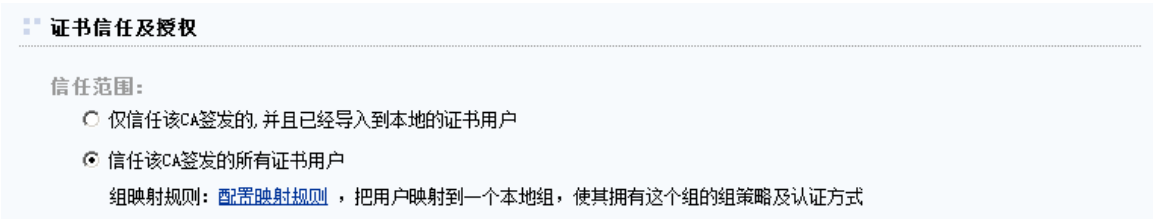
OID：与 DN 类似，通常需要填写存放用户名等唯一标识用户的 OID 属性。

[证书编码]用于设置此证书使用的编码格式。

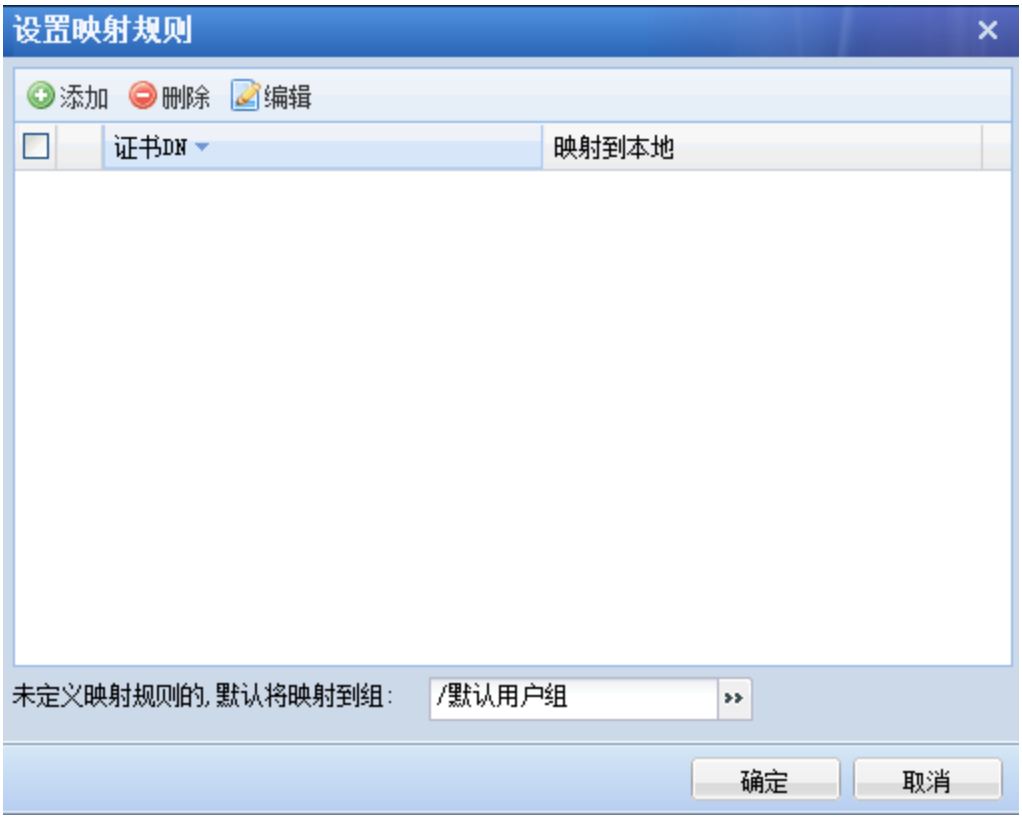


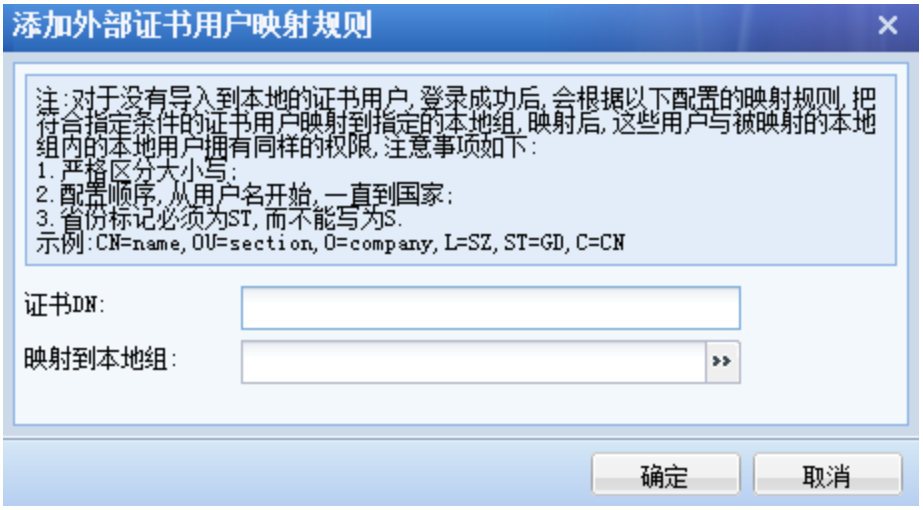
选择『仅信任该 CA 签发的，并且已经导入到本地的证书用户』，则只有当用户证书被导入到 VDC 网关，用户才能通过该用户证书登录 VDI。

选择『信任该 CA 签发的所有证书用户』，则只要是 CA 颁发的有效用户证书，都允许登录 VDI。配置页面如下：



点击配置映射规则用于设置将特定某证书 DN 映射到 VDI 本地用户组，使这些证书用户登录 VDI 之后自动分配到该用户组，并拥有该用户组的权限。设置页面如下：





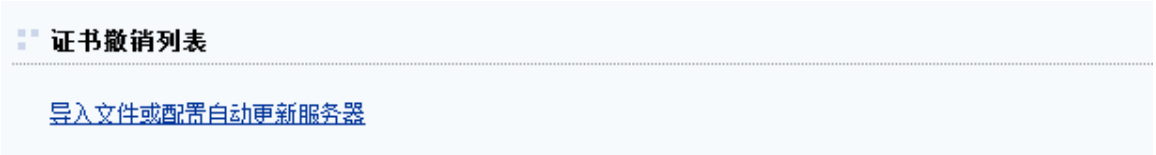
『证书 DN』可以通过证书主题查看。

『映射到本地组』用于设置拥有该字段证书登录后映射到的用户组。

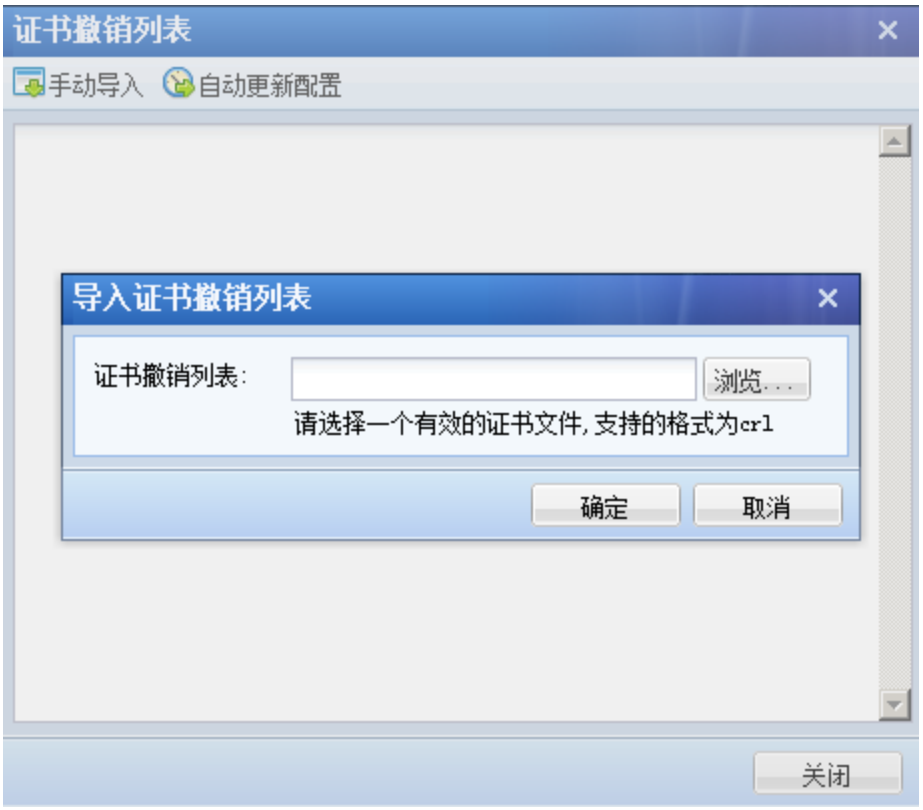
点击删除，可以删除选中的映射规则。

点击编辑，可以编辑选中的映射规则。

『未定义映射规则的，默认将映射到组』用于设置对于没有做映射规则的证书，登录 VDI 后默认被分配到哪个用户组。

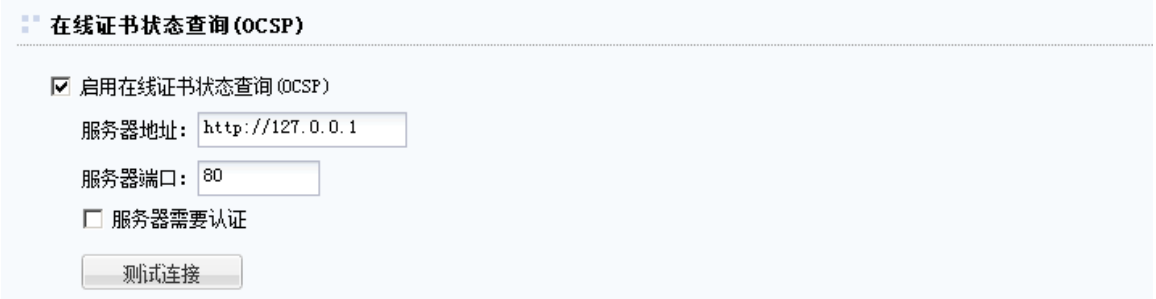


点击导入文件或配置自动更新服务器，可以手动更新或配置自动更新证书撤销列表，撤销列表支持格式为：*.crl。配置页面如下图：



选择相应的证书吊销列表文件进行导入，若选择自动更新配置，则弹出如下界面：

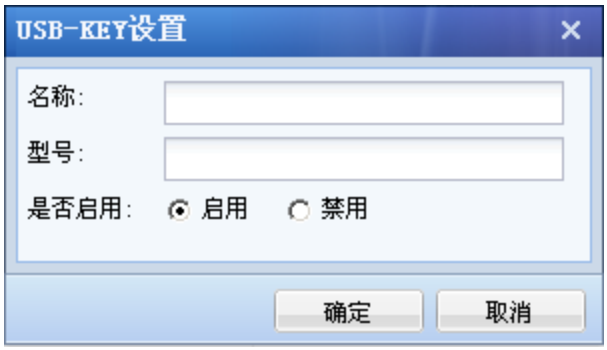
勾选[启用自动更新 CRL]并设置颁发点地址和更新频率。



[在线证书状态查询]用于实时的更新 CA 证书的状态。

『通用 USB-KEY 设置』用于配置支持第三方 USB KEY 的接入和拔出注销，配置好 USB KEY 的型号，当用户登录时，SANGFOR VDC 网关会检测 USB KEY 的型号，假如和我们设置的型号对应，那么当用户将 USB KEY 拔出时，用户将自动注销。配置如下图：

点击添加，配置页面如下：



『名称』自定义此设置的名称。

『型号』用于设置需要拔出 USB KEY 自动注销用户的 USB KEY 型号。

『是否启用』用于设置对该型号 USB KEY 启用或禁用拔出 KEY 自动注销功能。

点击确定，保存配置，并将配置添加到列表中。

点击删除，用于删除列表中的 USB KEY 信息。

点击编辑，用于编辑列表中的 USB KEY 信息。

4.7.1.5. 域单点登录认证

域单点登录认证用于解决客户端 PC 已经登录域的情况下，使用 C/S 登录客户端登录 VDI 时无需再输入用户名及密码，即可自动完成域认证，成功登录 VDI。域单点登录认证

只支持客户端方式的登录，不支持网页形式的登录。

WEBUI 路径：『VDI 设置』→『认证设置』→『主要认证』→『域单点登录认证』。页面如下：

点击域单点登录认证后面的设置，弹出【域单点登录认证设置】页面，如下图：

『域单点登录』勾选[启用]，启用域单点登录功能。

『服务器域名』用来设置 Windows 域的域名。

『域名简称』用来设置 Windows 域的域名简称。

『域控计算机全名』用来设置 Windows 域的域控制器名称。

『域控 IP 地址』用来设置 Windows 域的域控制器的 IP 地址。

『域管理员名』用来设置登录 Windows 域的管理员帐号。

『域管理员密码』用来设置登录 Windows 域的管理员密码。

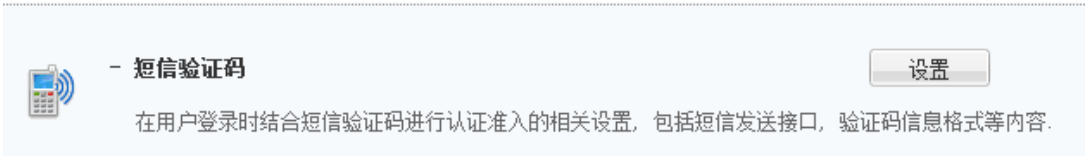
4.7.2. 辅助认证

『辅助认证』包含『短信验证码』、『硬件特征码』、『动态令牌认证』。点击『短信验证码』、『硬件特征码』、『动态令牌认证』的设置出现相关认证的设置页面。

4.7.2.1. 短信验证码

『短信验证码』即 VDI 用户登录时，输入用户名/密码后，VDC 网关会使用发送短信的方式向该用户的手机号码发送一个动态生成的随机密码，即短信验证码，登录用户必须输入该验证码，才能成功登录 VDI，访问内网资源。

WEBUI 路径：『VDI 设置』→『认证设置』→『辅助认证』→『短信验证码』。页面如下：



点击设置，弹出【短信认证设置】页面，如下图：

『短信验证码』用于设置启用或禁用短信认证功能。

『重新发送间隔』用于设置短信发送间隔时间。

『验证码有效期』用于设定动态密码的有效时间，用户登录 VDI 时，如果输入的动态密码超过了有效时间，则登录失败，需要重新获取验证码。可定义时间为 1－1440 分钟。

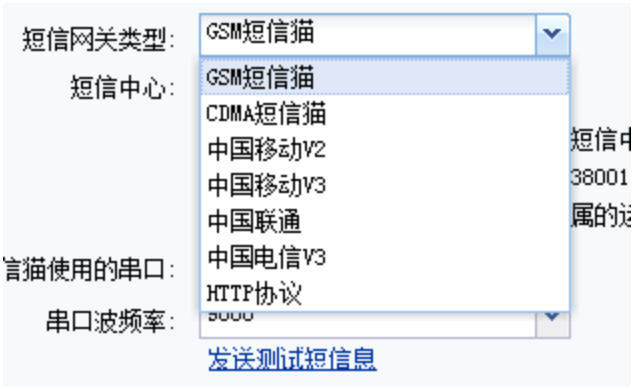
『自定义短信』用于设定发送到客户端手机上短信的内容。

点击恢复默认格式，可以将自定义短信的内容恢复为默认值。

『短信验证码发送模块选择』包括[通过设备内置短信模块发送]和[通过安装在外部服务器上的短信模块发送]两种方式。配置如下图：

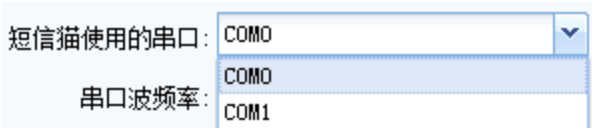
『短信发送参数』用来配置发送短信的参数，配置如下图：

『短信网关类型』用来配置发送短信的网关类型，可以选择通过[GSM 短信猫]（接到短信模块服务器 com 口）、[CDMA 短信猫]、[中国移动 V2]、[中国移动 V3]、[中国联通]、[中国电信 V3]和[HTTP 协议]的短信网关发送。

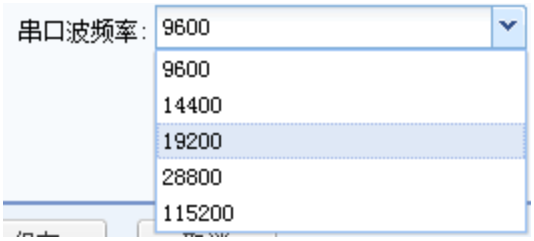


『短信中心』短信猫所对应的运营商的短信中心号码。

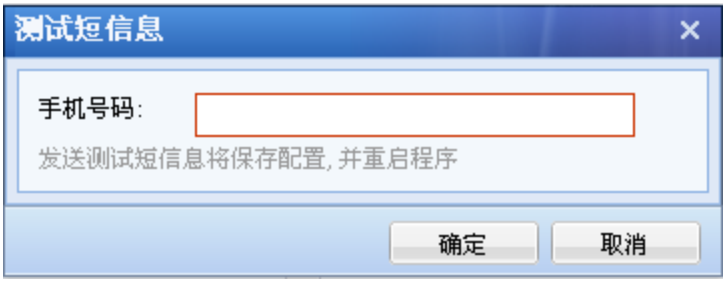
『短信猫使用的串口』即短信猫所使用的串口。可选择[COM0]和[COM1]，如下图：



『串口波频率』VDC 设备和相连的短信猫通讯的波特率，可选择五种波频率，一般用默认的 9600 即可。



点击发送测试短信息，出现测试短信息的设置页面：



『测试短信息』是用于测试短信猫或者短信网关能否正常发送短信，填入接收短信的手机号码，点击确定，发送测试短信。

要配置短信验证码，需要先开通短信认证序列号（可参考 3.1.1“序列号管理”章节）否则会有如下提示：

点击点击这里，可以跳转到『序列号管理』页面。

通过设备内置短信模块发送

[通过设备内置短信模块发送]表示使用 VDC 设备自带的短信中心模块功能。

短信网关类型选择『短信猫』，那么除了 VDC 设备，还需要准备的硬件有短信猫和电话卡。

第一步：将一手机 sim 卡放入短信 Modem 内；

第二步：通过发货时自带的串口线（一端为公头，另一端为母头）将短信猫连接到 VDC 设备后面的 CONSOLE 口上，注意把接口上的旋钮扭紧，确保串口线和短信 Modem 以及串口线和短信服务器接触良好。

第三步：『短信发送参数』中『短信网关类型』选择[GSM 短信猫]。

第四步：『短信发送参数』中『短信中心』为当地短信服务运营商的短信服务号码，例如深圳的为：8613800755500。

第五步：『短信网关配置』中『短信猫使用串口』选择[COM0]。

第六步： 『短信发送参数』中[串口波频率]为 VDC 设备和相连的短信猫通讯的波特率，一般为 9600，可根据所使用的短信 modem 实际参数进行设置。

第七步：点击保存，配置完成。

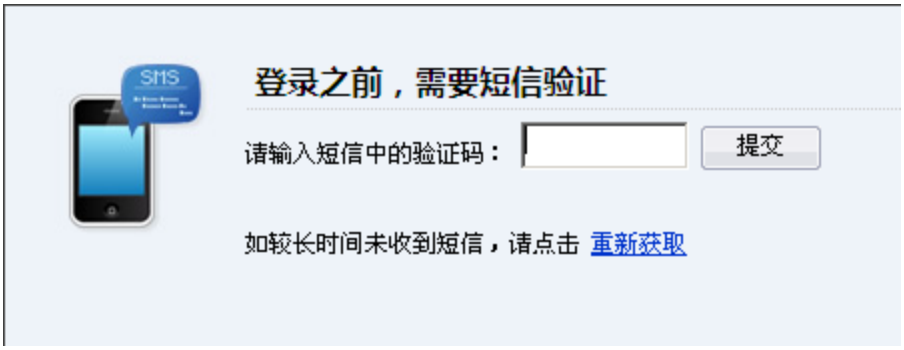
如下图所示：

第八步：对用户启用短信认证；

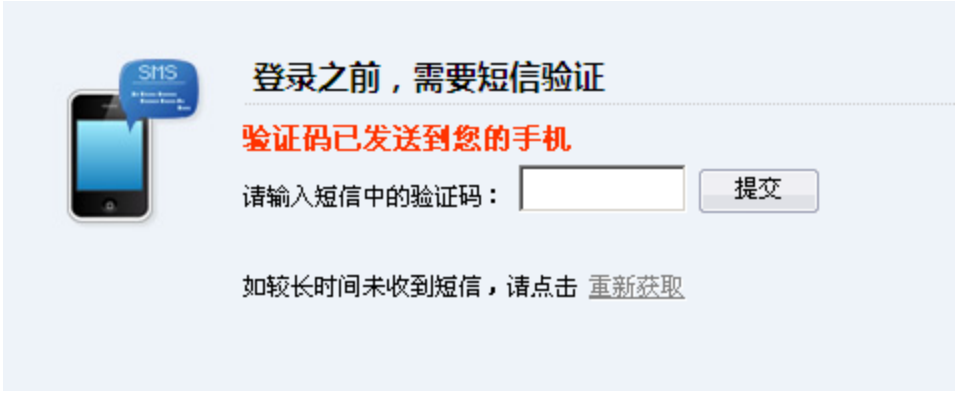
注意：必须填写用户的手机号码；『账户类型』必须勾为[私有用户]；『辅助认证』必须勾选短信认证；如上图红色框标注部分。

第九步：登录 VDI。首先输入用户名和密码，点击登录按钮，会弹出短信认证的页面。

如下图所示：



输入手机收到的短信检验码，点击提交即可。如果没有收到短信，可以点击重新获取按钮。



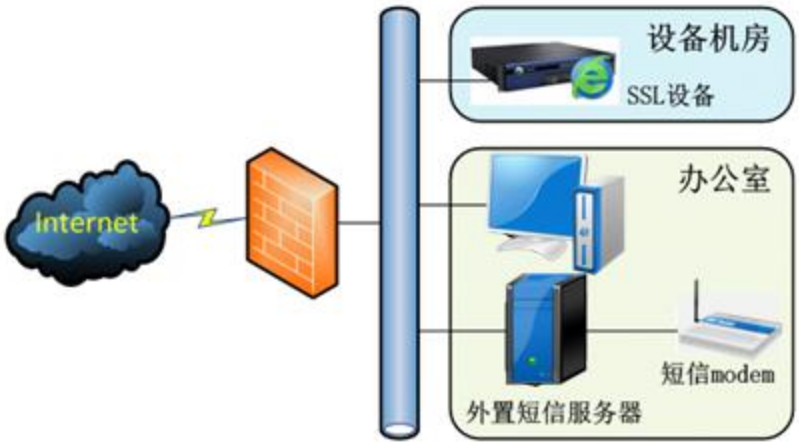
通过安装在外部服务器上的短信模块发送

[通过安装在外部服务器上的短信模块发送]即短信模块安装在某一台服务器上，通过短信服务器来发送短信；短信网关类型可以选择[GSM 短信猫] /[CDMA 短信猫]/[中国移动 V2]/[中国移动 V3]/[中国联通]/[中国电信 V3] /[HTTP 协议]。

以短信猫为例说明『外置短信模块』的使用方法。构建短信服务器只需要一台主板上带有 com 口的电脑，并且安装上深信服公司提供的短信服务软件即可。

支持系统：Windows XP、Windows 2000、Windows 2003，不支持 vista 系统。

外置短信模块结构图：



第一步：将一手机 sim 卡放入短信 Modem 内；

第二步：短信 Modem 通过发货时自带的串口线（一端为公头，另一端为母头）连接到短信服务器（电脑）的 com 口上，注意把接口上的旋钮扭紧，确保串口线和短信 Modem 以及串口线和短信服务器接触良好；

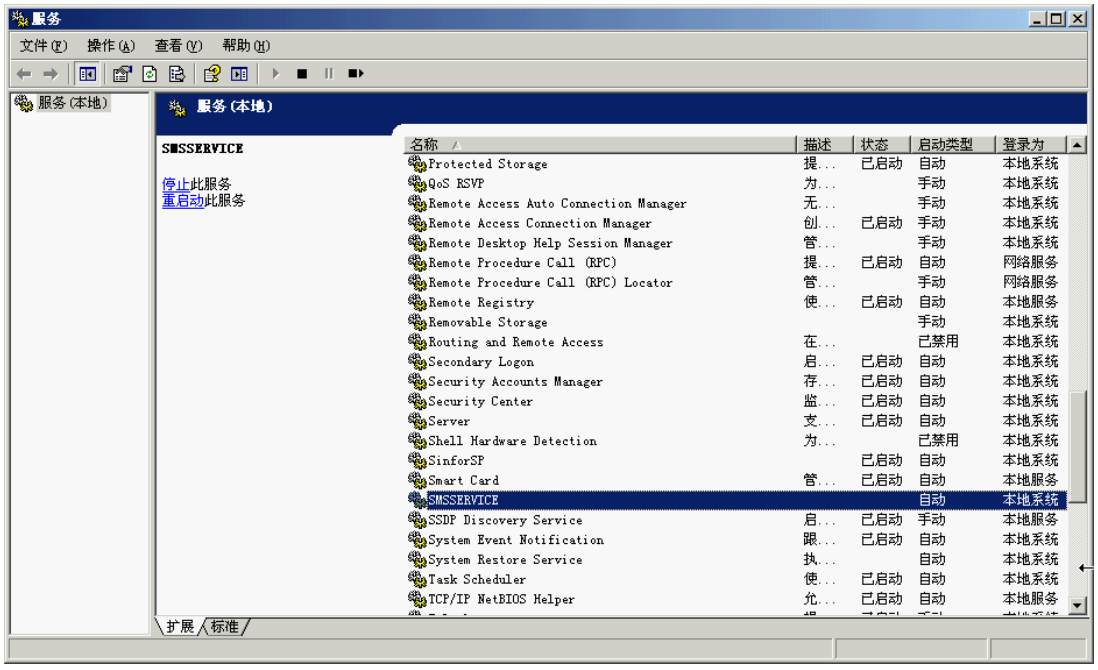
第三步：在短信服务器上安装深信服提供的软件安装包；

第四步：软件安装完成后，短信服务会以系统服务的形式自动运行，短信服务进程为“SMSSP.exe”；

如下图所示：

在服务列表中能够看到短信服务“SMSSERVICE”；

如下图所示：



在系统的“开始”菜单打开短信服务软件的控制台，进行配置

在系统桌面右下角的控制台能够看到当前短信服务的状态，左图为服务正常，右图为服务异常

如果软件安装好后，服务仍然显示停止，一般情况下是由于软件没有安装在系统盘下造成的，请把软件重新安装在默认路径下。

第五步：鼠标右键点击控制台，选择“Config”

在软件服务的监听端口设置对话框里，设置好监听端口（TCP 端口），如果服务器还提供其他服务，可以使用 netstat –na 查看服务器上已监听的端口，要保证设置的端口和这些服务的端口不冲突

如果短信服务器上装有防火墙软件，必须保证防火墙有放通此处设置的短信服务监听端口。

至此“外置短信服务器”设置完毕。

第六步：登录 VDC 设备的控制台，打开『VDI 设置』→『认证设置』→『短信验证码』，配置短信认证信息。

配置如下图所示：

『短信中心地址』填上短信服务器的 IP，必须保证 VDC 设备能够和短信服务器正常通信（VDC 设备能够连通短信服务的监听端口）。

『短信中心端口』填上短信服务软件的监听端口。

『短信网关类型』下拉框，选择[GSM 短信猫]。

『短信中心』填写短信 Modem 上所放入的 sim 卡的短信中心号码，根据 sim 卡的实际情况填写（可咨询 sim 卡的服务提供商）。

『短信猫使用的串口』根据实际情况填写，目前一般电脑只有一个 com 口，选则“0”就可以了，若接到第二个 com 口上，则选择“1”。

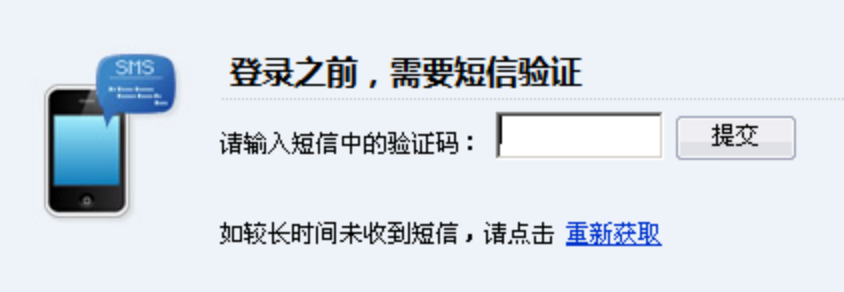
『串口波频率』下拉框选择[9600]。

第七步：对用户启用短信认证；

注意：必须填写用户的手机号码；『账户类型』必须为[私有用户]；『辅助认证』必须勾选短信认证；如上图红色框标注部分。

第八步：登录 VDI。首先输入用户名和密码，点击登录按钮，会弹出短信认证的页面。

如下图所示：



输入手机收到的短信检验码，点击提交即可。如果没有收到短信，可以点击重新获取按钮。

使用运营商短信网关

如果网络中已经有中国移动短信网关或者中国联通短信网关，可以和 VDI 结合使用。配置方法如下：

『短信网关类型』中选择[中国移动 V2]/[中国移动 V3]/[中国联通]/[中国电信 V3]。

如果启用『外置短信模块』，『短信模块设置』中『短信中心地址』填写短信模块软件服务器的 IP，『短信中心端口』填写短信模块软件实际监听的端口。

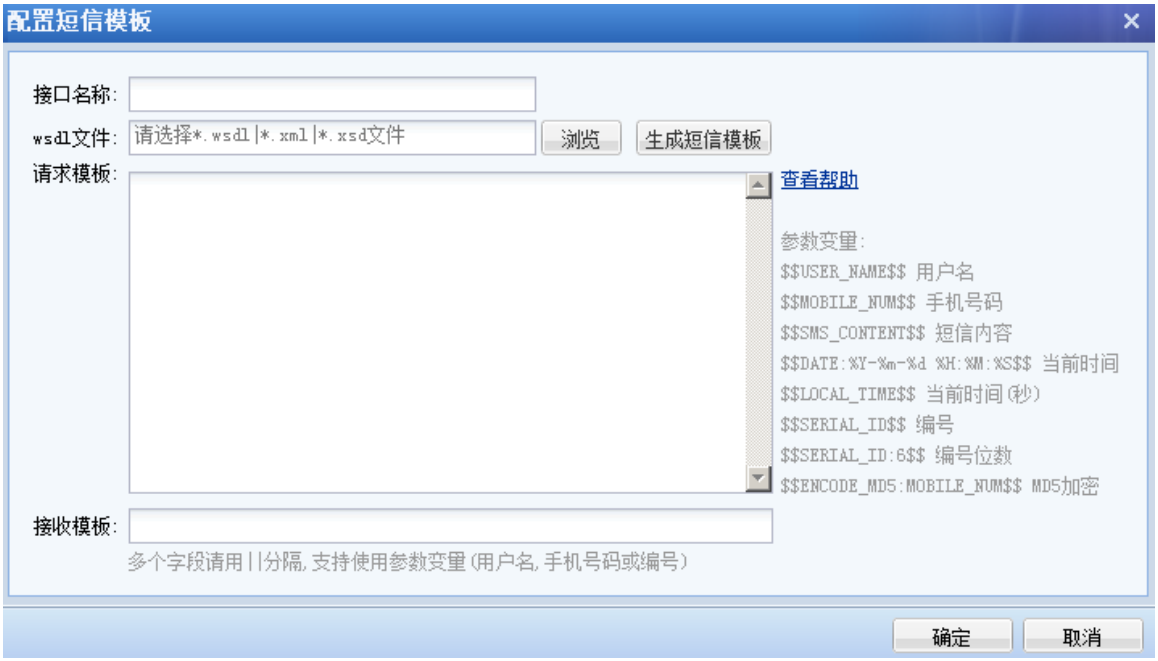
『短信发送参数』中的剩余的『短信网关服务器地址』、『短信网关服务器端口』、『企业代码』、『业务代码』、『SP 接入号』、『网关编号』、『登录帐号』、『登录口令』、『确认口令』信息请按照短信服务提供商提供的相关参数填写。

使用 webservice 方式发送短信校验码

VDC 设备可以与基于 webservice 的短信平台联动，支持以 webservice 方式发送短信校验码，保障加强短信发送的稳定性。配置界面如下：

『短信网关类型』中选择 HTTP 协议，设置 webservice 短信网关平台的地址，页面编码方式以及 SOAP 版本和请求类型。

点击配置短信模板用于设置短信模板的接口名称等信息。

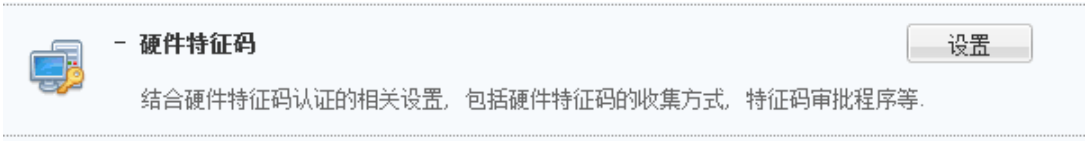


4.7.2.2. 硬件特征码

『硬件特征码』根据计算机的硬件特性按一定的算法生成的一个序号，由于硬件特性的唯一性，使得该硬件特征码也是唯一的、不可伪造的，所以对于不同的计算机，此序号必然不同。

『硬件特征码』用于对用户的硬件特征码权限进行设置。

WEBUI 路径：『VDI 设置』→『认证设置』→『辅助认证』→『硬件特征码』。页面如下：



点击设置，弹出【硬件特征码认证设置】页面，如下图所示：

[启用硬件特征码收集]选择此项，则设备只收集用户登录的硬件特征码，但不会启用硬件特征码认证。

[启用硬件特征码认证]选择此项，则开启硬件特征码认证。

『自定义提示信息』提示用户提交硬件特征码时的用语。

[自动审批]勾选此项后，用户提交的硬件特征码不需要管理员手工审批，可自动通过审批。

[所有已审核的终端上，允许任意账号登录]勾选此项后，如果某一用户使用的计算机提交了硬件特征码并通过了审批，则其他用户用此计算机登录所提交的硬件特征码可自动通过审批。

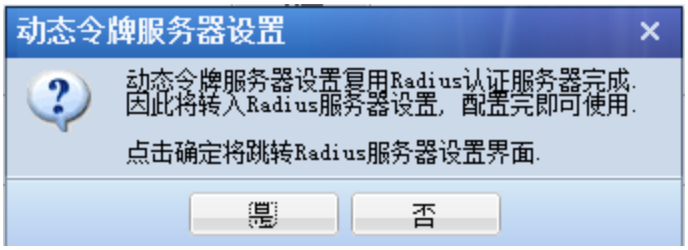
点击保存使配置生效。

4.7.2.3. 动态令牌认证

『动态令牌认证』是 Radius 服务器的一种扩展使用，通过与 Radius 服务器结合并为用户配发动态令牌，通过动态令牌上的动态密码进行登录，由此增加登录的安全性。

WEBUI 路径：『VDI 设置』→『认证设置』→『辅助认证』→『动态令牌认证』。页面如下：

点击动态令牌认证的设置按钮，出现动态令牌服务器设置框如下：



点击是，跳转到 Radius 认证服务器管理页面，详细配置请参照 4.7.1.3 章节。

4.7.3. 认证选项设置

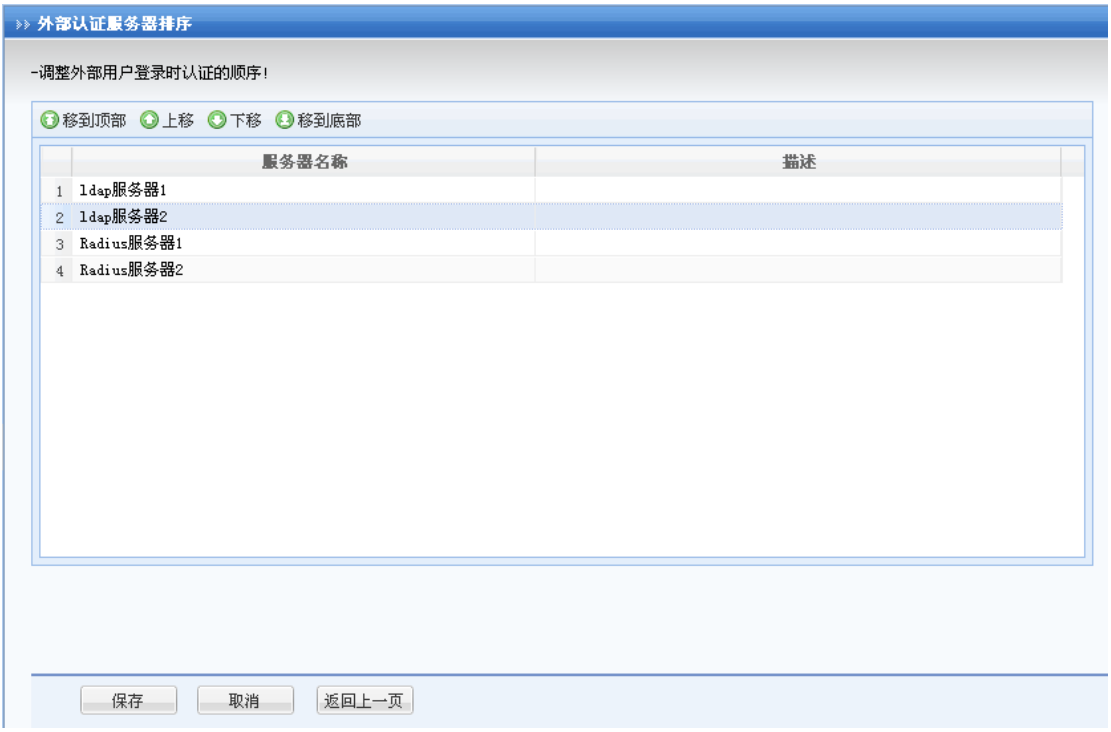
『认证选项设置』包含『LDAP 与 Radius 服务器认证优先级设置』、『密码认证选项』和『匿名登录设置』。

4.7.3.1. LDAP 与 Radius 服务器认证优先级设置

『LDAP 与 Radius 服务器认证优先级设置』用于设置用户通过外部服务器中的用户名密码认证时，到各个服务器中认证的优先级。

WEBUI 路径：『VDI 设置』→『认证设置』→『LDAP 与 Radius 服务器认证优先级设置』，页面如下：

点击设置，弹出【外部认证服务器排序】页面，如下图：



【外部认证服务器排序】用于对设置好的 LDAP 和 Radius 服务器进行排序，当外部认证用户登录时，先到第一个服务器中认证，当第一个服务器中无此用户时，再到第二个服务器中认证，以此类推。

选中某台服务器，点击移到顶部、上移、下移、移到底部，可对服务器进行相应的

排序。

点击保存，完成并保存配置。

4.7.3.2. 密码认证选项

『密码认证选项』用于设置当用户通过用户名密码方式认证登录 VDI 时的一些相关选项设置。

WEBUI 路径：『VDI 设置』→『认证设置』→『密码认证选项』，如下图：

点击设置，弹出【密码认证选项设置】页面，包含『用户登录时校验选项』和『防止暴力破解选项』，如下图：

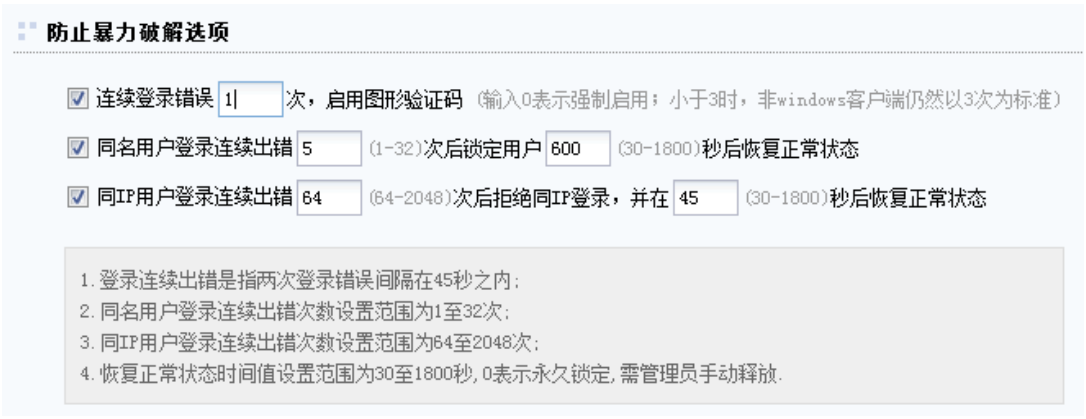
『用户登录时校验选项』的配置页面如下：

勾选[启用软键盘]，可以在 VDI 登录页面启用软键盘和图形校验码，增强登录的安全性。勾选[启用软键盘]并勾选[数字顺序变化]或[字母顺序变化]则每次登录时数字顺序或字母顺序都会改变。如下图所示：

勾选『启用软键盘』，打开登录页面：

点击密码输入框后的小键盘图标，页面如下：

『防止暴力破解选项』是一种安全机制，可设置用户用相同用户名连续输错多少次密码则冻结该用户，该用户在一段时间内将无法登录；或者用户用相同一个 IP 地址连续输错多少次密码，则启用图形校验码或者锁定该 IP 一段时间。配置如下图所示：



图形验证码选项设置中，输入 0 表示强制启用，即默认启用图形验证码；输入小于 3 时，非 Windows 客户端仍然以 3 次为标准。

当客户登录 VDI，连续输错 5 次密码即锁定用户，结果如下图所示。

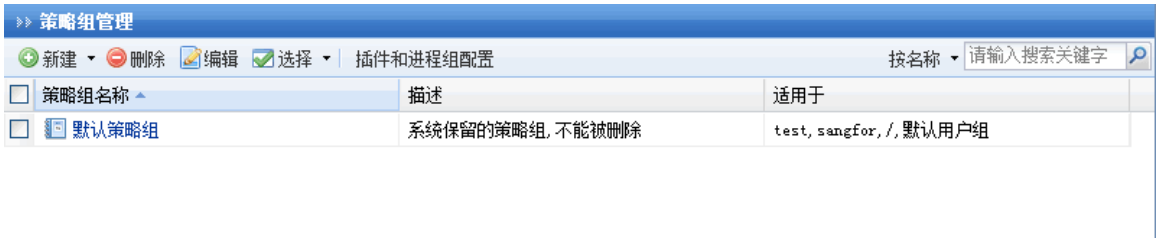
当设置同 IP 连续输错 64 次密码后启用图形校验码认证，VDI 客户端同一个 IP 连续输错 64 次密码之后，结果如下图所示。

当设置同 IP 连续输错 64 次密码后暂时拒绝同 IP 登录，VDI 客户端同一个 IP 连续输错 64 次密码之后，结果如下图所示。

4.8. 策略组管理

『策略组管理』用于配置客户端相关选项、账号控制、安全桌面及远程应用等。

WEBUI 路径：『系统菜单』→『VDI 设置』→『策略组管理』。界面如下图所示：



『策略组名称』显示策略组的名称。

『描述』用来显示策略组的描述信息。

『适用于』显示引用该策略组的用户/用户组。

点击新建，选择新建策略组，用来新建策略组。

点击新建，选择以所选策略组为模板新建，用来以已经存在的策略组作为模板来新建一个策略组。使用此功能必须要先勾选一个策略组。

点击删除，用来删除勾选的策略组。

点击编辑，用来编辑勾选的策略组。

点击全选，用来选择当前页或所有页的策略，也可以取消选择，如下图：

查询中可选择[按名称]、[按描述]或[按适用范围]来查找策略组。在输入搜索关键字中输入相应的关键字，点击后面的即可。

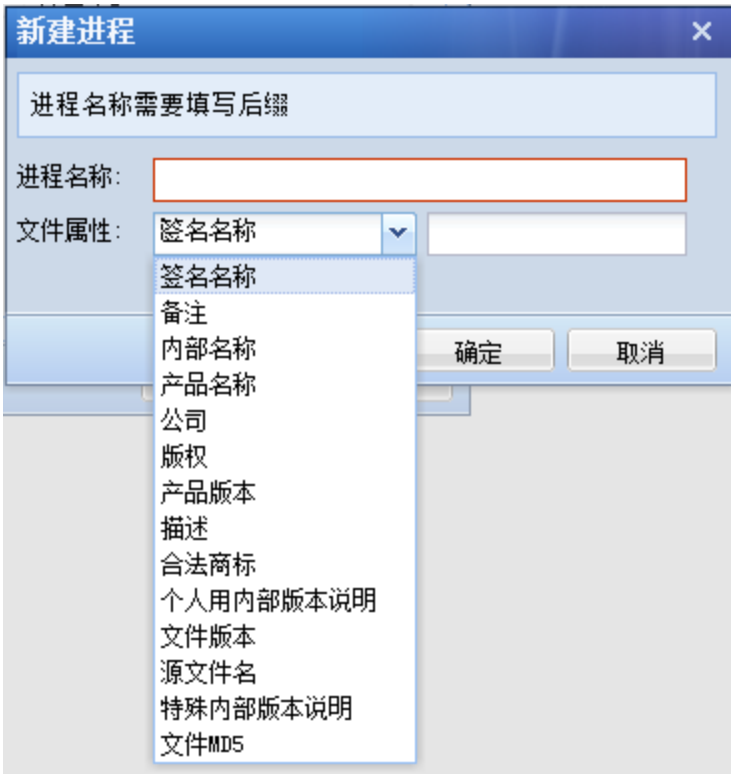
点击进程和插件组配置用于设置需要在安全桌面策略组内引用的进程和插件组。

『插件列表』点击新建按钮，填写需要在安全桌面内放行的插件名称。

[文件名称]填写插件的名称。

[签名名称]填写插件的签名者。

『进程组列表』点击新建按钮，填写需要在安全桌面内放行的进程名称。



点击新建，选择新建策略组，弹出【新建策略组】页面。界面如下图所示：

『名称』定义策略组的名称。

『描述』填写策略组的描述信息。

『策略选项』用来设置客户端选项、账号控制、安全桌面和远程应用。

设置完策略组之后，需要在『用户管理』里将策略组关联给用户或用户组，如果不进行关联的话，即使设置了也是没有作用的。

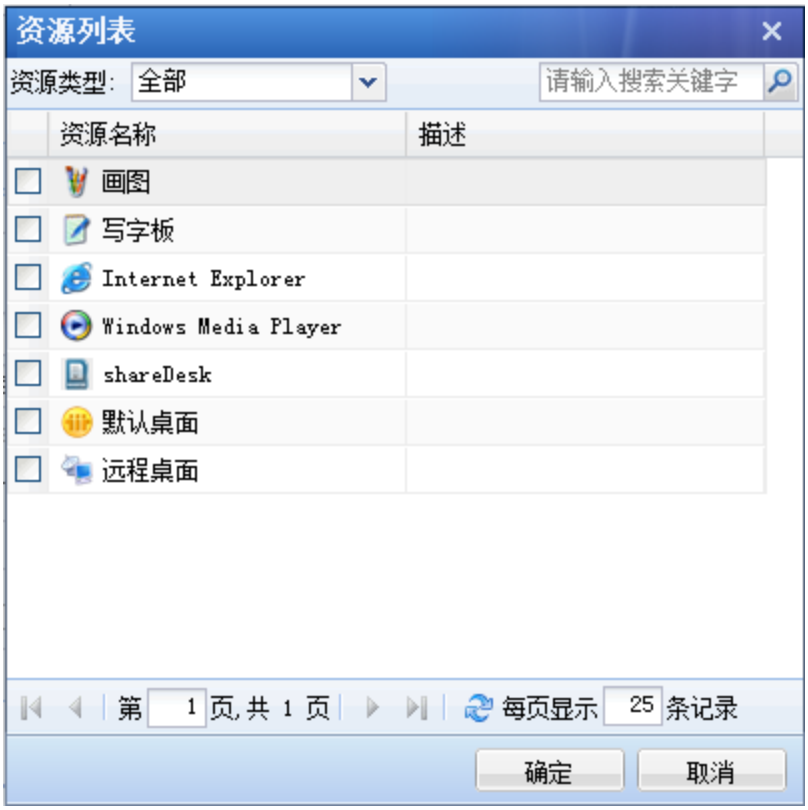
4.8.1. 账号控制

『账号控制』用来设置账号控制选项、私有用户权限等信息。界面如下图所示：

『账号控制选项』用来设置记录用户访问日志、启用系统托盘、用户登录后跳转到指定资源、限制用户可访问时段、用户闲置失效时间、用户超时时间。

[记录用户访问日志]若勾选，可以在外置数据中心记录下该用户访问 VDI 的所有日志。

[用户登录后跳转到指定资源]设置用户登录 VDI 后默认跳转到指定的资源，点击[用户登录后跳转到指定资源]后，弹出【资源列表】页面，可选择具体的资源。注：必须先设置好相应的资源（资源的具体设置可参考 4.5『资源管理』章节）。界面如下图所示：



『限制用户可访问时段』用来限制接入 VDI 的时间，点击『限制用户可访问时段』的下拉列表框选择相应的时间。注：必须先设置好相应的时间（时间的具体设置可参考 3.6『时间计划』章节）。

[用户闲置 XX 天后失效]用来设置用户 XX 天没有登录 VDI 后，将账号自动禁用。可以手动设置天数。

[用户如果 X 分钟内未进行任何操作则自动断开连接]用来设置用户超时时间，当用户达到设置的时间未进行过任何操作时，则将用户自动断开连接。设置时间范围 5-43200 分钟。

『允许私有用户自行修改以下信息』用来设置是否允许私有用户修改密码、修改描述和修改手机号码。界面如下图所示：

勾选即允许修改。勾选后，如果用户类型是私有用户，登录 VDI 后，便可以点击资

源列表页面右上方的『设置』，左边列表中选择『账号信息』来修改密码、用户描述和手机号码，如下图：

如果要修改手机号码，必须先对该用户启用短信认证。

完成配置后，点击保存，最后在策略组管理界面点击配置生效，保存配置并生效。

4.8.2. 独享桌面

『独享桌面』用来设置独享桌面用户相关的策略控制。如下图：

『剪切板』勾选后表示启用 windows 客户端剪切板功能，下拉列表框可选择“允许虚拟桌面与真实桌面双向拷贝”，“只允许从虚拟桌面拷贝到真实桌面”，“只允许从真实桌面拷贝到虚拟桌面”三个选项。不勾选“剪切板”表示不启用 windows 客户端剪切板功能，此时对应组策略的用户将无法使用该功能。

『USB 存储器』勾选后表示可以使用 USB 存储类设备，USB 存储器数据访问权限的下拉列表框可选择“允许读写 USB 存储器”，“只允许读 USB 存储器”。若不勾选“USB 存

储器”，则表示无法使用 USB 存储类设备。

『允许使用 USB 打印机』勾选后表示支持使用 USB 接口的打印机设备，若不勾选，则不允许使用。

『USB 设备加载到本地桌面』勾选后允许 USB 设备加载到本地桌面，即在开启 VDI 时，PC 端真实桌面可以使用 USB 设备，若不勾选，则 PC 端默认不能使用 USB 设备（鼠标键盘类设备除外）。

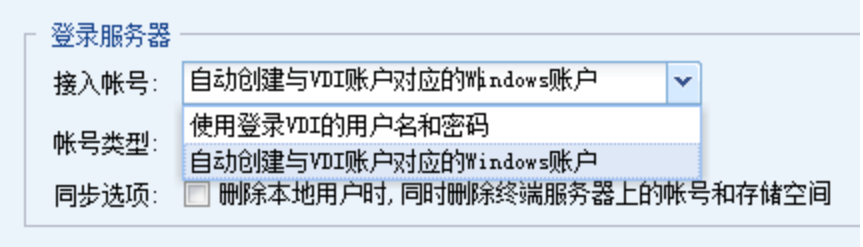
『允许使用串口』勾选后表示可以使用串口设备，若不勾选，则不允许使用。

『隐藏导航条』勾选后表示可以隐藏瘦客户机导航条。

4.8.3. 远程应用与共享桌面

『远程应用与共享桌面』用来设置登陆终端服务器、在远程会话中允许使用的设备和资源、服务器数据安全、终端存储目录、和终端服务访问权限。如下图：

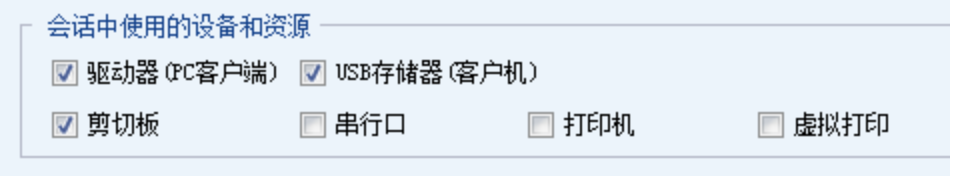
『接入帐号』选择移动用户使用什么账号权限登录终端服务器。如下图：



『账号类型』根据上面选择的账号策略在终端服务器上自动创建的 Windows 账号的类型 。

『同步选项』，勾选[删除本地用户时，同时删除终端服务器上的账号和存储空间]即当删除了关联该策略组的本地用户时，将该策略组在终端服务器上建立的账号和存储空间一并删除。

『会话中使用的设备和资源』中，可以选择在远程会话中允许使用的设备和资源。若不勾选，则不允许使用。如下图：



『驱动器（PC 客户端）』勾选后，用户可以在访问远程应用资源时打开或将文档保存到本地磁盘。

『USB 存储器（客户机）』勾选后，用户可以在远程应用资源中访问客户端的 USB 存储器。

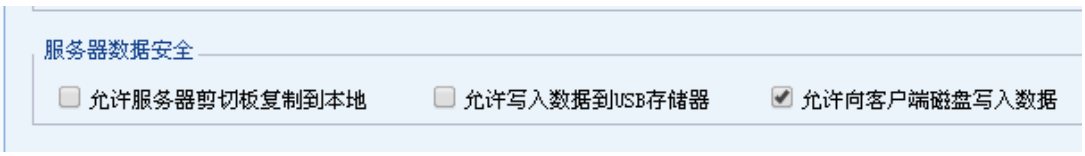
『剪切板』勾选后，表示启用 windows 客户端剪切板功能。

『串行口』勾选后，表示可以使用串口设备。

『打印机』勾选后，用户在服务器上安装打印机驱动以后，可以使用客户端打印机打印远程应用中的文档。

『虚拟打印』勾选后，用户可以通过在服务端选择 Sangfor 虚拟打印机，在客户端本地打印机打印文件，且终端服务器无需安装本地打印机驱动。

『服务器数据安全』针对远程应用服务器的安全配置项。页面如下：



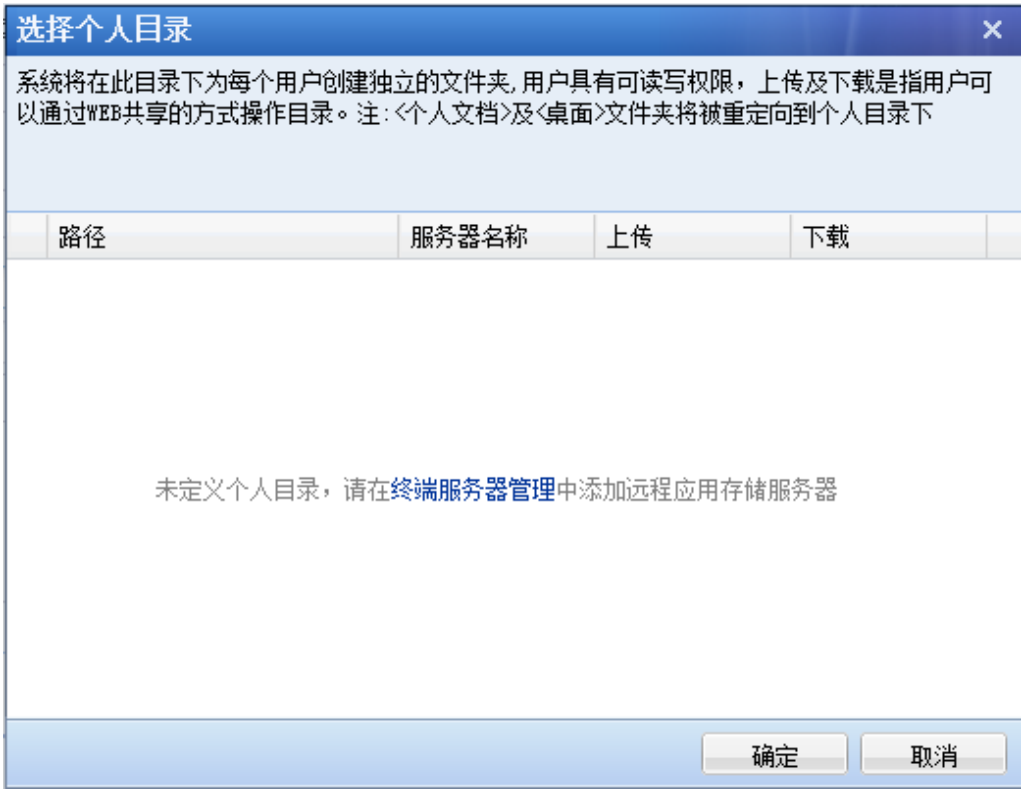
『允许服务器剪切板复制到本地』若勾选则可以从服务端的远程应用或者共享桌面中使用剪切板拷贝数据到真实桌面，若不勾选则默认禁用。

『允许写入数据到 USB 存储器』若勾选则表示可以允许往映射到服务器端的 USB 存储器设备写数据，若不勾选则只能读数据。

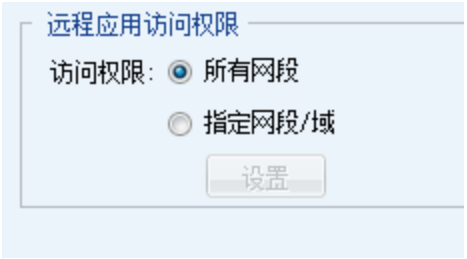
『允许向客户端磁盘写入数据』若勾选则表示允许磁盘映射功能的写入功能，若不勾选则不能写入，只能读取。

『远程存储目录』用来选择需要在远程服务器上存储文件的目录，包括[个人目录]和[公共目录]。页面如下：

点击后面的  ，可以选择相应的目录，选择之前，需要先在服务器管理中添加相应的远程应用存储服务器，详细配置请参考 4.3 章节。



『远程应用访问权限』为不同用户配置不同的放行网段或者放行域名，对用户关联的所有远程应用的网络访问进行限制。允许访问的网段可选择所有网段或指定某一个网段/域，页面如下：



选择[指定网段/域]，点击设置，可手动配置一段 IP 或指定一个域名，如下图：

以上所有配置完成后，点击保存，最后在策略组管理界面点击配置生效，即完成了一条策略组的添加。

4.9. 端点安全

VDC 网关提供一种检测机制，能够保证客户端计算机符合管理员指定的安全策略时才允许接入，例如可以指定客户端必须运行某杀毒软件、防火墙，必须是哪一种操作系统，必须打什么补丁等。

WEBUI 路径：『VDI 设置』→『端点安全』。如下图

分为“用户登录前检查”和“用户登录后定时检查”。

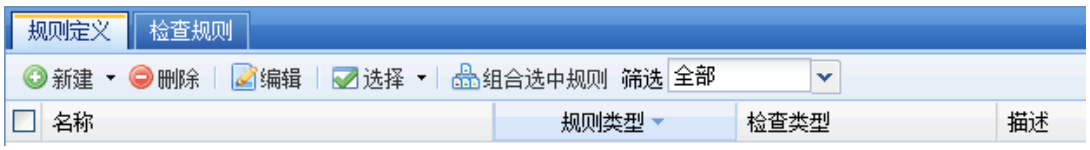
“用户登录前检查”：用户进入 VDI 登录页面，检查是否满足登录前安全策略组，若不满足，则拒绝接入。

“用户登录后定时检查”：用户登录后，根据“角色”应用不同策略组，定时检查（间隔由管理员指定），若不满足，则拒绝提供服务。

4.9.1. 端点安全规则

『端点安全规则』用来定义端点安全规则设置规则检查策略。

WEBUI 路径：『VDI 设置』→『端点安全』→『端点安全规则』。如下图：



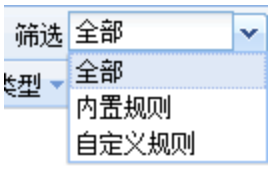
点击删除，用来选择所选择的规则。

点击编辑，用来编辑一条所选的规则。

点击全选，可选择当前面或所有页，也可以取消选择。

点击组合选中的规则，可以将所选择的基本规则组合在一起，新建一条组合规则。使用此功能前必须要先选中需要组合的规则才可以。该功能与在【规则定义】页面点击新建，选择组合规则，然后添加所需要组合的规则实现效果是一样的。

点击『筛选』后的下拉框，选择需要在列表中显示的规则，包括：[全部]、[内置规则]、[自定义规则]。如下图：

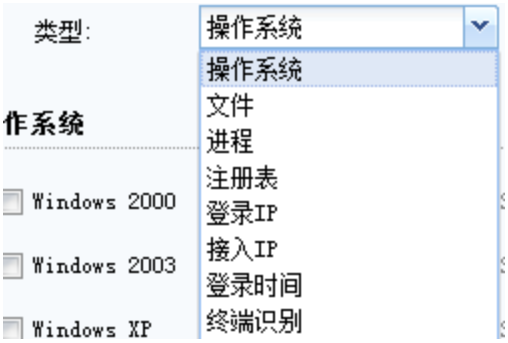


点击新建，可新增[基本规则]或[组合规则]，如下图：

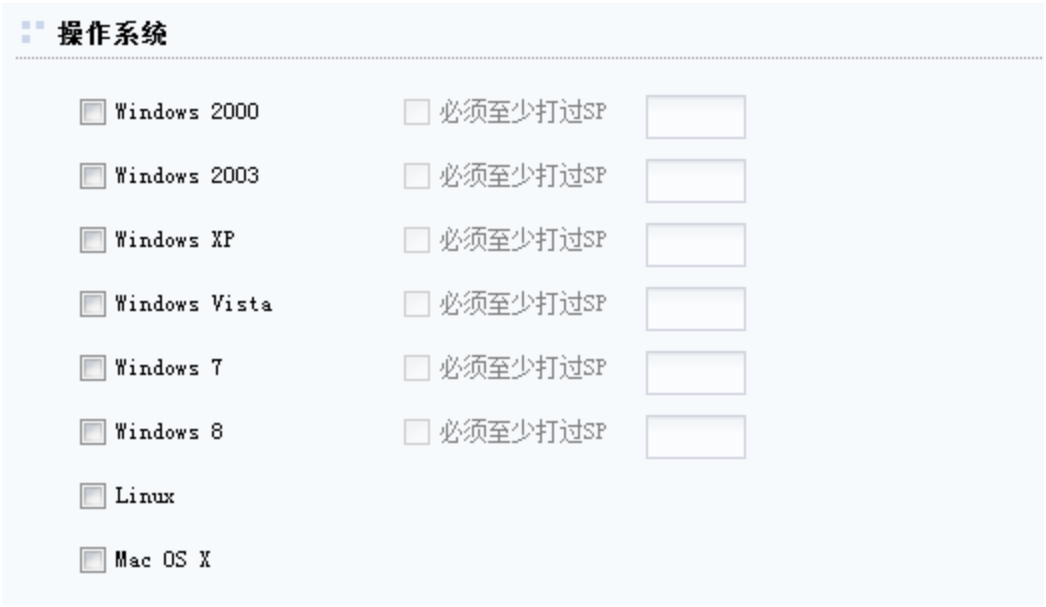
选择基本规则，用来新建一条端点安全基本规则。如下图：

『规则名称』和『规则描述』可随意填写便于理解记忆的文字。

『类型』可选择[操作系统]、[文件]、[进程]、[注册表]、[登录 IP]、[接入 IP]、[登录时间]、[终端识别]。如下图：



1>[操作系统]类型，配置对话框如下：



选择相应的操作系统后，后面可再勾选附加条件，该操作系统至少打过 SPX 的补丁。

注意：系统的类型可以多选，之间是“或”的关系，系统后面的『必须至少打过 sp』项是对该系统的一个补充。

2>『文件』类型，配置对话框如下：

[用户 PC 必须存在本文件]选择后登录 VDI 的客户端计算机硬盘上必须存在该文件，才满足该规则。

[用户 PC 不能存在本文件]选择后登录 VDI 的客户端计算机硬盘上不存在该文件，才

满足该规则。

『文件路径』填写指定文件的在客户端计算机的路径，可以使用绝对路径或使用系统变量（如%SystemRoot%\log.txt）。

注意：『文件』下填写的字母区分大小写，该项为必填项。

『更新日期比当前日期滞后不大于 XX 天』所指定的文件最后更新的日期不能落后客户端计算机系统时间的天数。

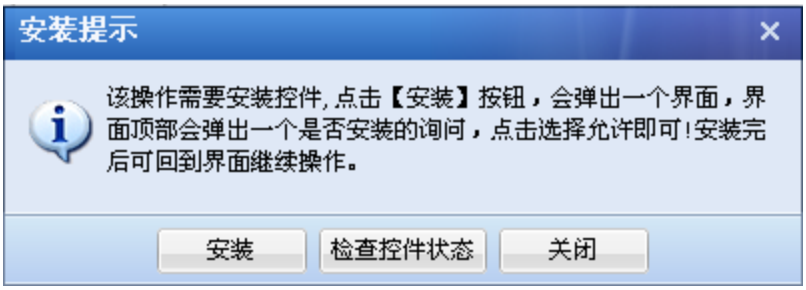
『文件 MD5』勾选后即可激活该项，点打开选择『文件』所填写的文件，即可获得该文件的 MD5 值，用于保证客户端计算机上的文件和管理员设置要求的文件内容完全相同。

『文件大小』勾选后即可激活该项，点打开选择文件，即可获得该文件的大小值，用于保证客户端计算机上的文件和管理员设置要求的文件大小完全相同。

注意：1.以上各项的配置是“与”的关系，只有以上条件全部匹配才能满足此规则。

2.第一次使用『文件 MD5』或『文件大小』功能时，设备会检测客户端是否有安装 WebUICtrl 这个控件，如果没有安装，则会弹出”安装提示”。

页面如下所示：



点击安装，则弹出 IE 安全告警提示安装控件。页面如下所示：

点击安装。

如果浏览器未提示安装控件，可以通过点击下载安装，手动执行安装控件。页面如下所示：

3>『进程』类型，配置对话框如下：

[必须已运行本进程]选择后登录 VDI 的客户端计算机必须存在该进程，才满足该规则允许接入；否则禁止接入。

[必须未运行本进程]选择后登录 VDI 的客户端计算机必须不存在该进程，才满足该规则允许接入。

『进程名』填写指定进程的进程名。

『窗口名』填写运行指定进程的程序的窗口名。

『文件 MD5』勾选后即可激活该项，点打开选择运行指定进程的程序文件，即可获得该文件的 MD5 值，用于保证客户端计算机上的程序文件和管理员设置要求的程序文件内容完全相同。

『文件大小』勾选后即可激活该项，点打开选择运行指定进程的程序文件，即可获得该文件的大小值，用于保证客户端计算机上的程序文件和管理员设置要求的程序文件大小完全相同。

注意：以上各项的配置是“与”的关系，只有以上条件全部匹配才能满足此规则。

4>『注册表』类型，配置对话框如下：

[用户注册表需存在下面的内容]选择后登录 VDI 的客户端计算机的注册表必须存在该项，才满足该规则。

[用户注册表不能存在下面的内容]选择后登录 VDI 的客户端计算机的注册表不存在该项，才满足该规则。

『项』、『名称』和『值』，填写在注册表中显示的项，名称和值。

点击保存，即可完成基本规则设置。，

点击提交并继续添加，即保存的当前基本规则的设置，同时不返回『端点安全规则』页面，可继续添加规则。

点击取消，取消设置。

注意：以上各项的配置是“与”的关系，只有以上条件全部匹配才能满足此规则。

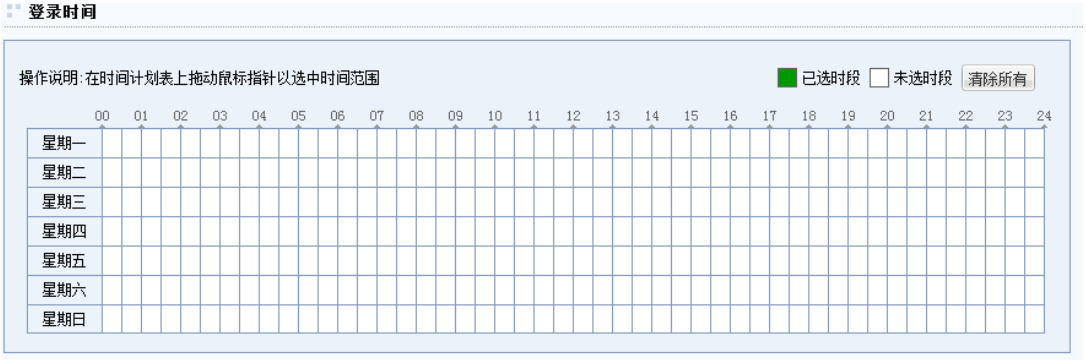
5>[登录 IP]类型，配置对话框如下：

『起始 IP』和『终止 IP』限制了客户端本身要处于某个 IP 地址范围才满足此规则。

6>[接入 IP]类型，配置对话框如下：

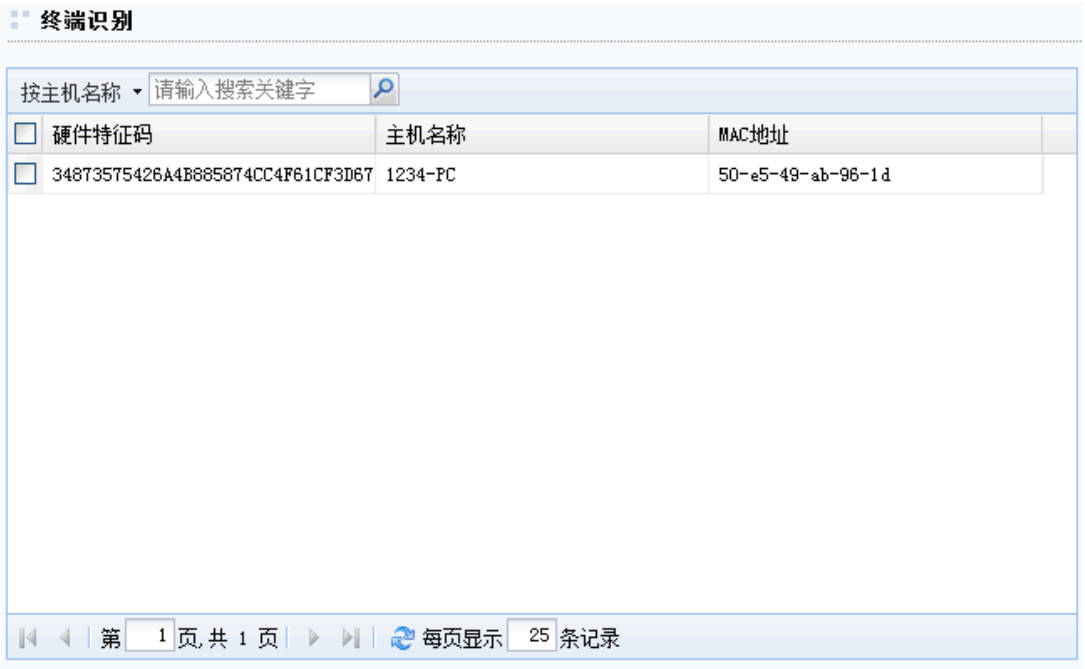
『接入 IP』中填写 VDC 设备某个接口的 IP 地址。设置了以后，只能通过该地址接入 VDI 才满足该条规则。

7>[登录时间]类型，配置对话框如下：



根据上面的时间小格定义时间段，具体设置方法可以参考章节 3.6 时间计划章节。

8、[终端识别]类型，配置对话框如下：



选择[终端识别]类型后，会在列表中列出硬件特征码管理中的硬件特征码，勾选上某个硬件特征码，点击保存完成该规则。当接入 VDI 客户端的硬件特征码属于此处勾选的其中一个时，则满足该规则，允许勾选多个硬件特征码。

硬件特征码可以通过[按主机名称]或[按 MAC 地址]查询。如下图：

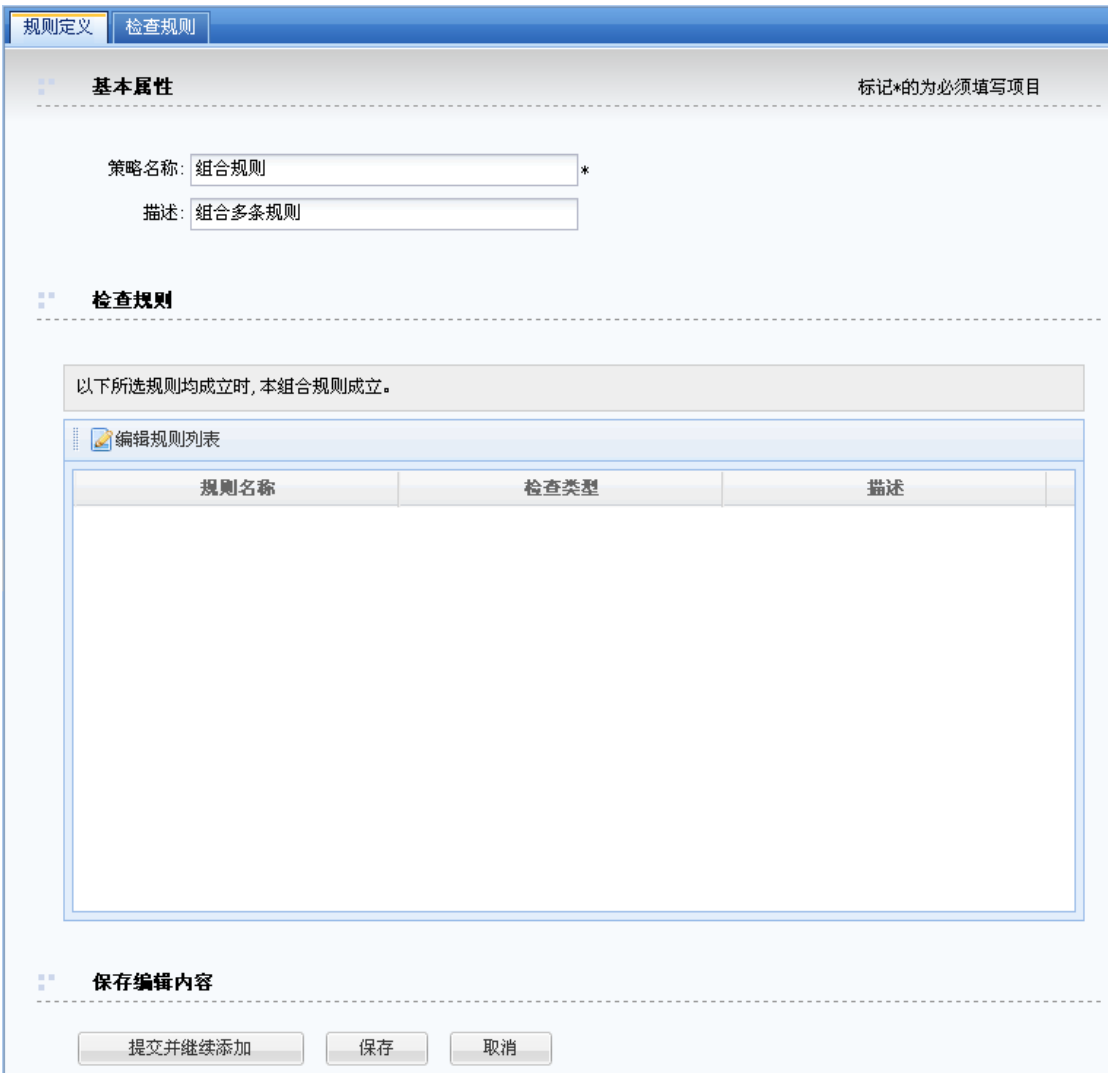
设置完基本规则后，点击保存，即可完成基本规则设置。

点击提交并继续添加，即保存的当前基本规则的设置，同时不返回『端点安全规则』页面，可继续添加规则。

点击取消，取消设置。

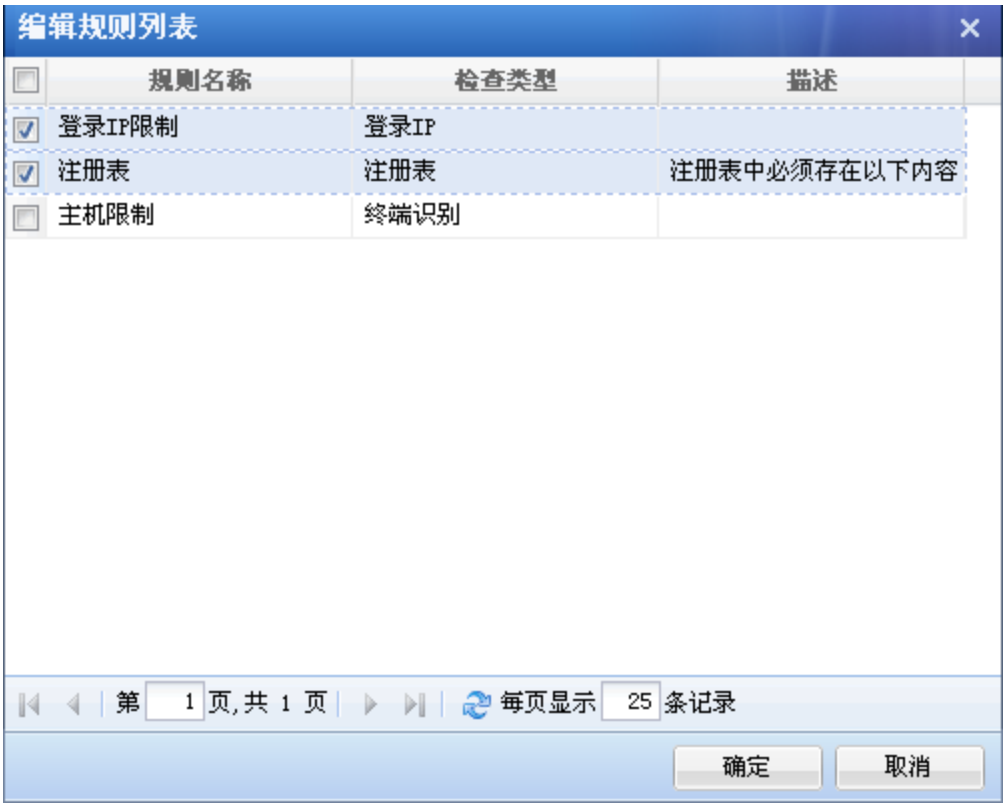
新建组合规则

在端点安全规则页面，点击新建，选择[组合规则]，新建一条组合规则，用来将多条基本规则结合使用。页面如下所示：



『检查规则』，点击编辑规则列表，弹出【编辑规则列表】对话框，可以选择需要组合的规则。

页面如下所示：



如上图，选择了[登录 IP 限制]和[注册表]两个规则，配置完成后，点击确定保存配置。

点击保存，即可完成基本规则设置。

点击提交并继续添加，即保存的当前基本规则的设置，同时不返回『端点安全规则』页面，可继续添加规则。

点击取消，取消设置。

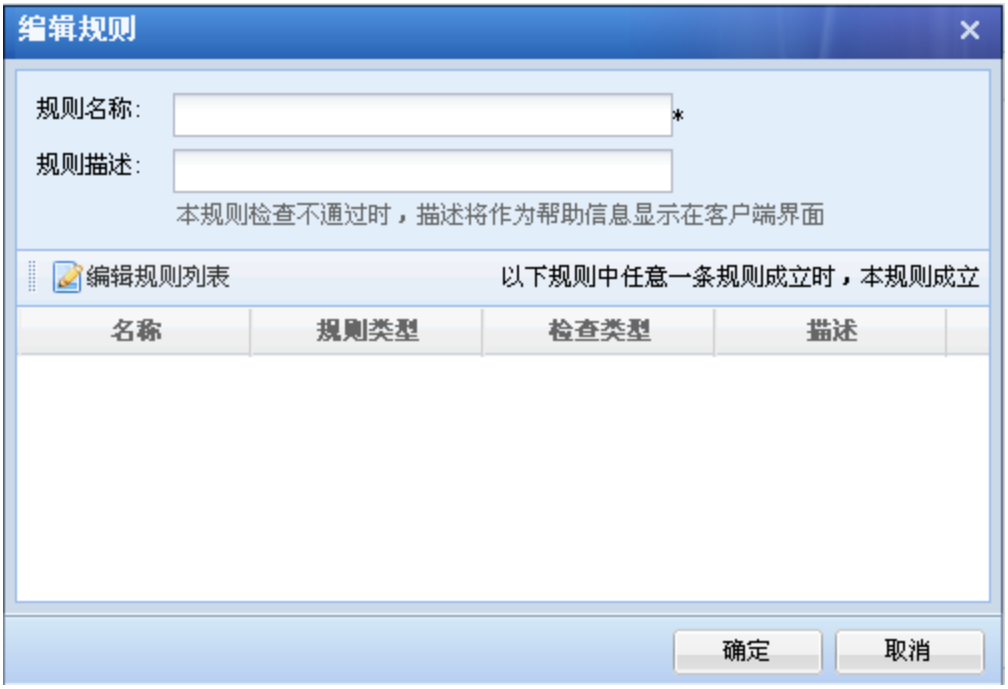
『检查规则』由若干“基本规则”或“组合规则”组合而成，只要策略中的任一个规则成立，则“检查策略”成立；规则都不成立时，“检查策略”不成立。

点击检查规则，用来新建端点安全检查规则。

页面如下所示：

点击新建，弹出『编辑规则』窗口，填写相应信息。

页面如下所示：



『名称』和『描述』可随意填写便于理解记忆的文字。

点击编辑规则列表，然后在『编辑规则列表』中勾选“基本规则”或“组合规则”，即可把“基本规则”或“组合规则”加入到该“检查规则”中，最后点确定保存配置。

注意：勾选多条规则，用户接入时任意一条规则成立，本规则便成立。

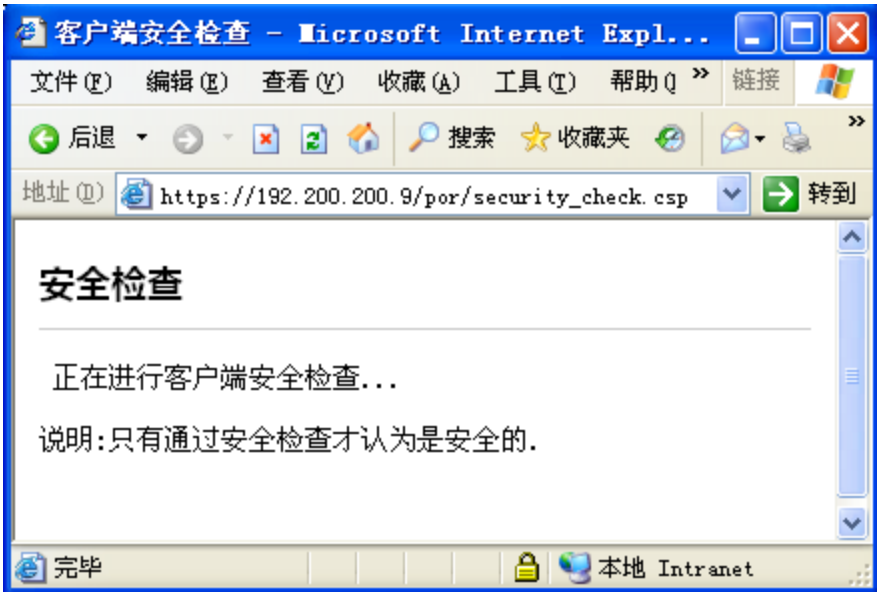
4.9.2. 端点安全策略

『端点安全策略』用来定义客户端登陆时的安全策略，包括接入准入策略，角色准入策略和客户端安全检查设置。

WEBUI 路径：『VDI 设置』→『端点安全』→『端点安全策略』。如下图：

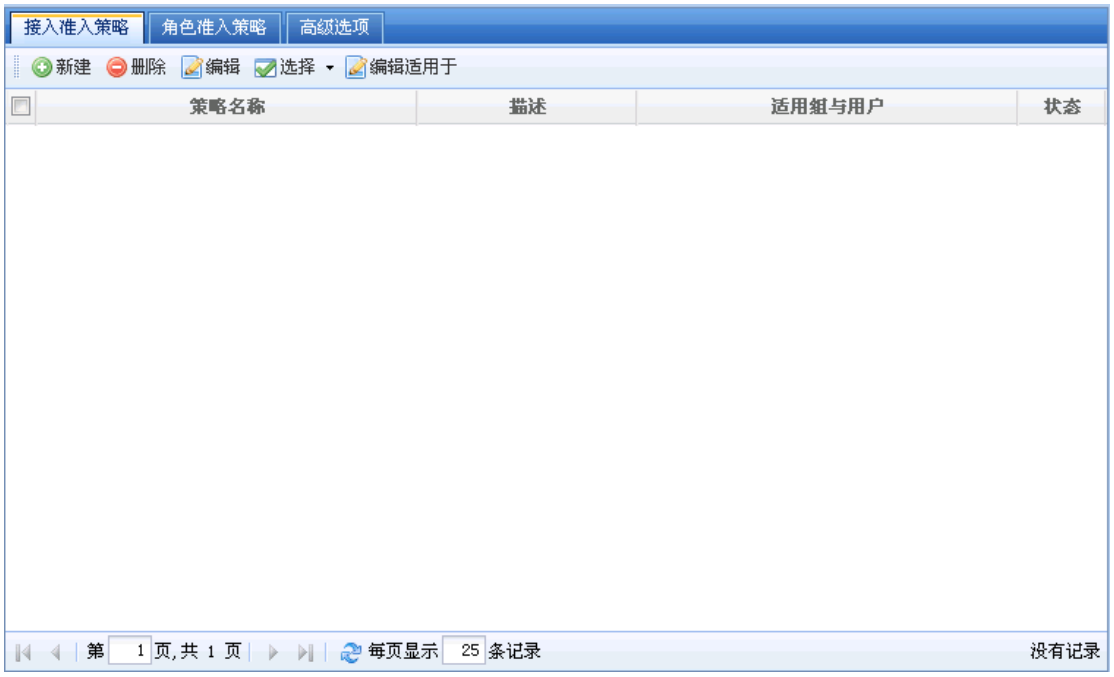
『端点安全策略』中定义“接入准入策略”，将检测规则与用户关联起来，实现用户接入访问时进行规则的检测。如果检测不通过，就会在页面左上角显示提示信息。

页面显示如下：



『编辑适用于』用来将『接入准入策略』和用户/用户组相关联。选择某一个接入准入策略，点击编辑适用于，选择相应的用户或用户组进行关联。

页面如下所示：

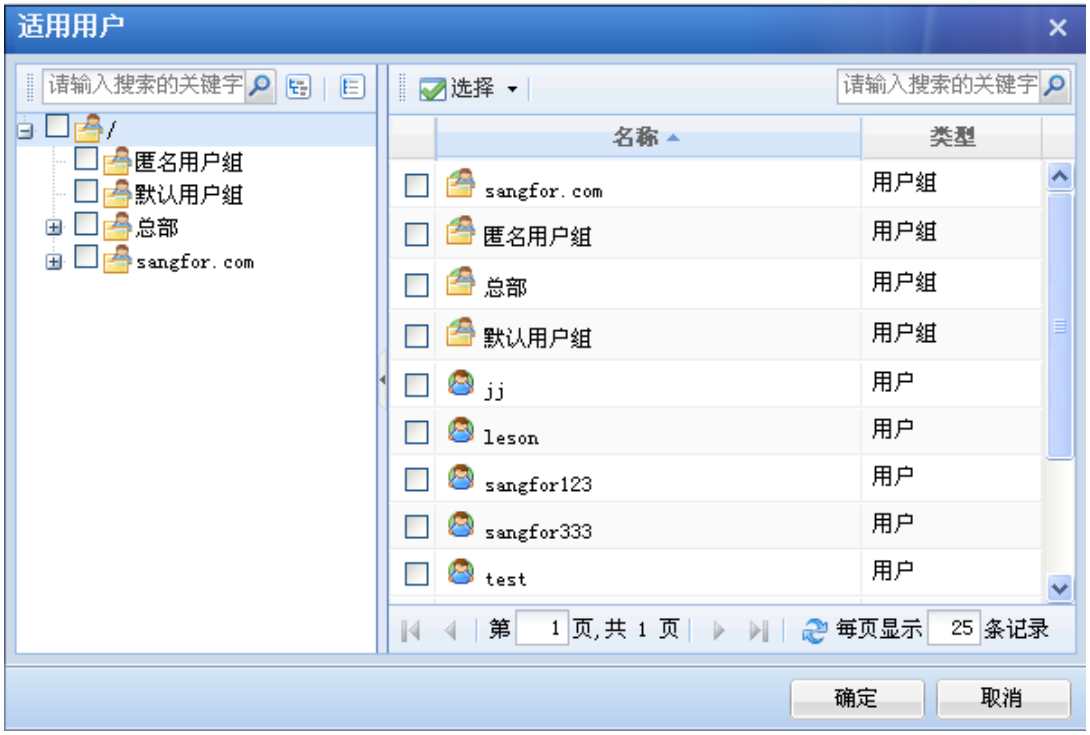


选择『接入准入策略』，点击新建，打开“接入准入策略”编辑窗口。页面所下所示：

『策略名称』和『描述』可随意填写便于理解记忆的文字。

『关联用户』用于选择将安全策略关联给某个用户或用户组，实现对该用户进行安全规则的检测。点击选择授权用户，打开【适用用户】窗口，选择用户或用户组。

页面如下所示：



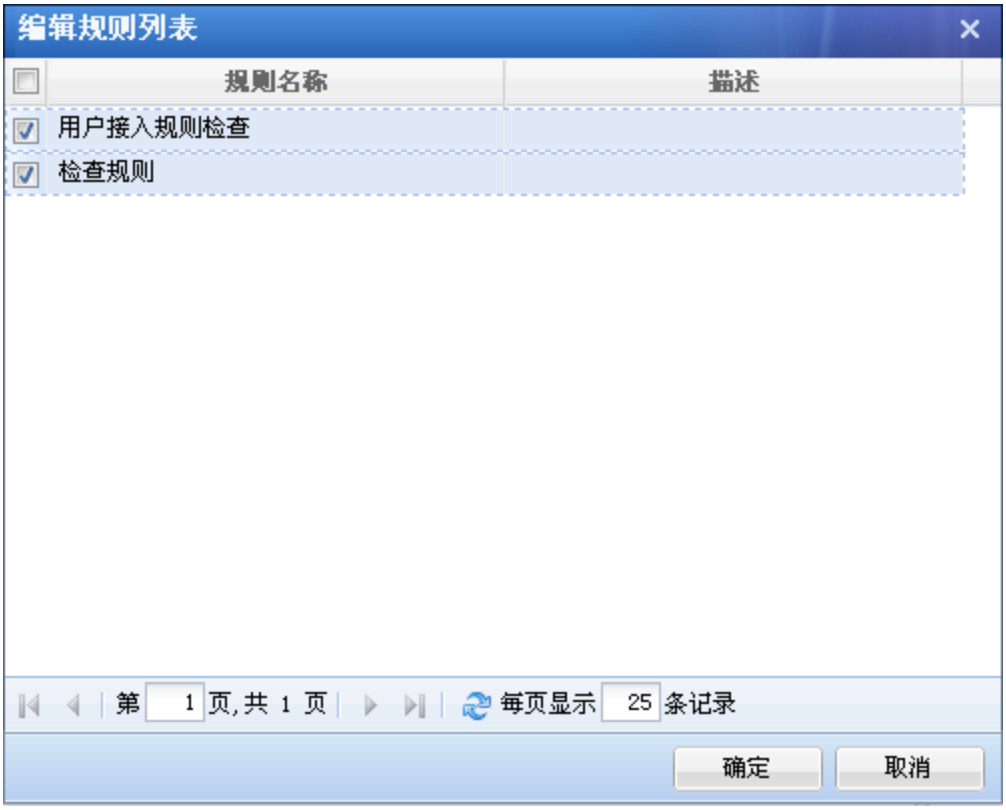
注意：这里所指的所选“用户组”是在左边用户组的选择，通过点击“用户组”的组名来选择的。

勾选[启用该策略]，启用本策略；不勾选，则禁用本策略。

『检查规则』用来设置『接入准入策略』关联的『检查规则』。实现将用户和『检查规则』相关联。

点击编辑规则列表，打开【规则编辑列表】，选择需要关联的检查规则。

页面如下所示：



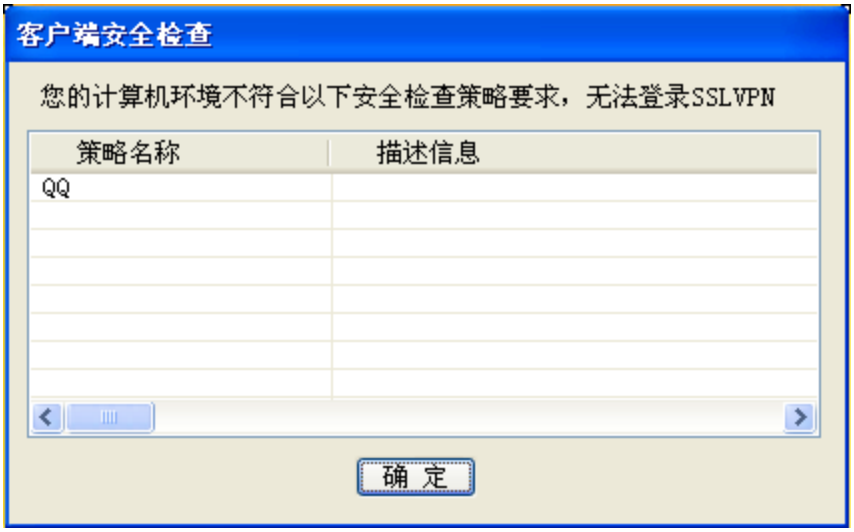
配置完成，点击确定，保存设置。

『角色准入策略』将检测规则与角色关联起来，实现与该角色关联的用户同时关联检测规则，用户接入访问时进行规则的检测。如果检测不通过，该用户将无法使用这个角色关联的资源，将资源放入『未获授权资源列表』。

页面显示如下：

用户登录后首先检查『接入准入策略』，如果『接入准入策略』没有通过，就会弹出提示不符合哪条安全策略。

页面显示如下：

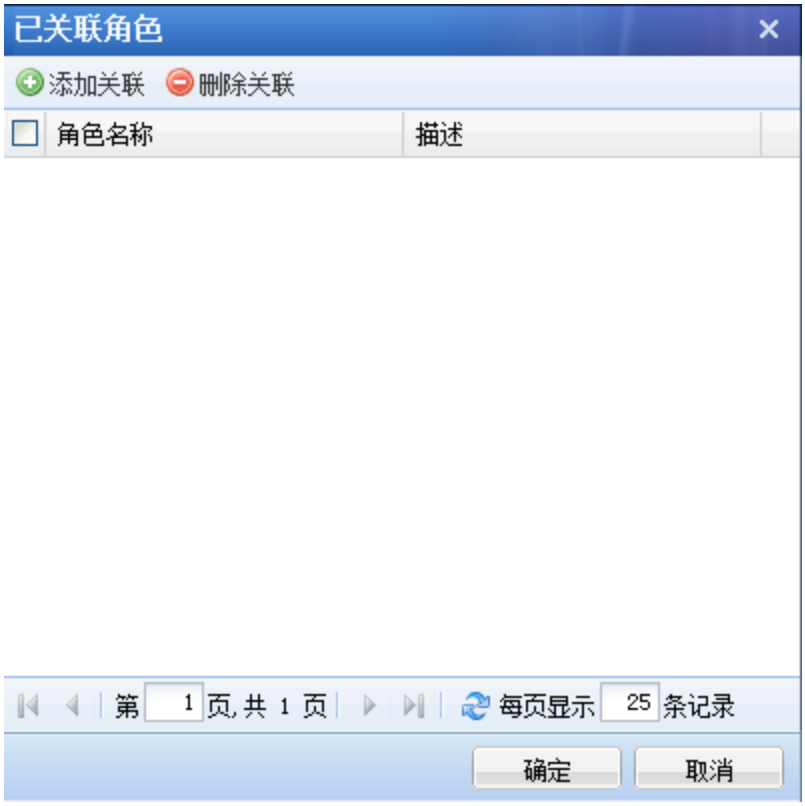


选择『角色准入策略』，点击新建，打开【角色准入策略】页面进行编辑。

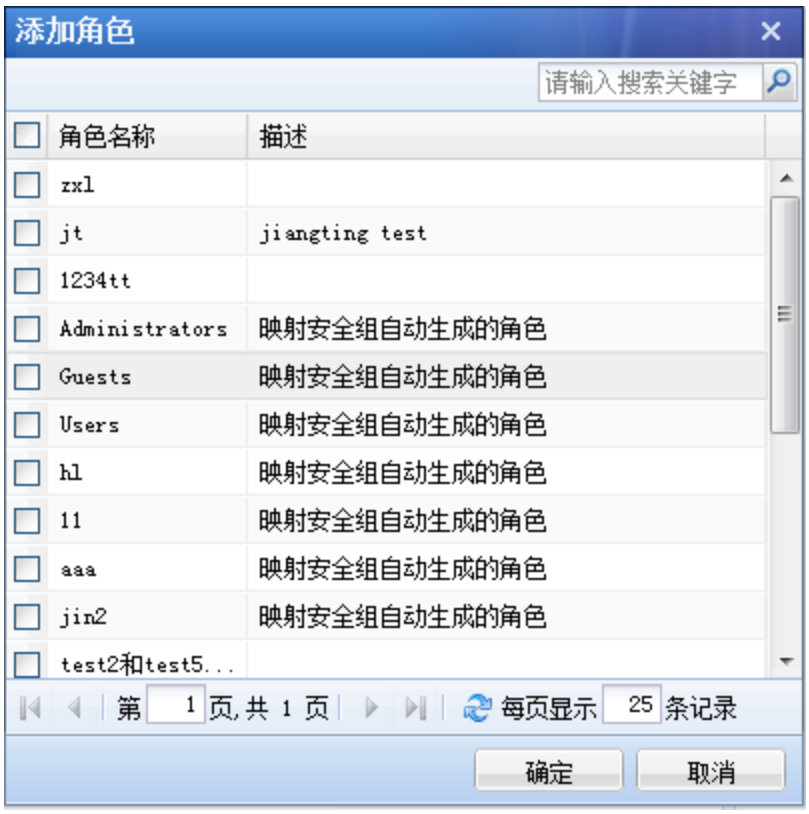
页面如下所示：

『策略名称』和『描述』可随意填写便于理解记忆的文字。

『关联角色』用于选择将安全策略关联给某个角色，实现对该角色所关联的用户或用户组进行安全规则的检测。点击选择关联角色，打开【已关联角色】窗口，选择角色进行关联。页面如下所示：



点击添加关联，打开【添加角色】窗口，勾选需要添加的角色。如下图：



配置完成，点击确定，保存设置。

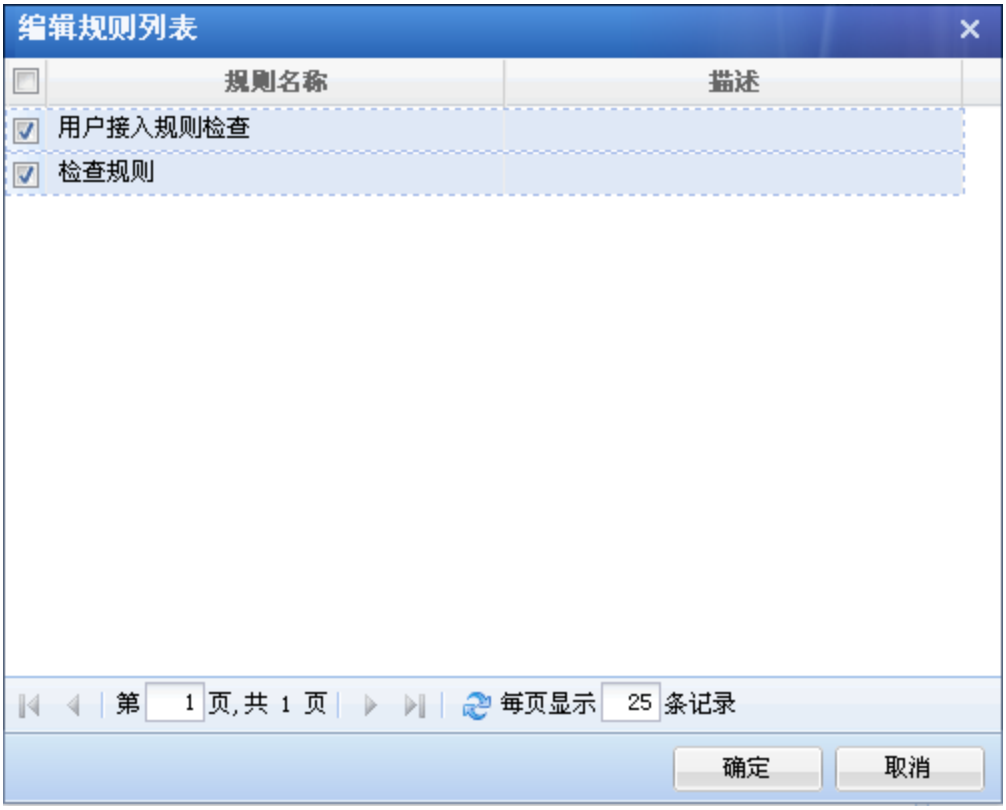
点击删除，删除所选角色。点击删除前勾选需要删除的角色。

配置完成，点击确定，保存设置。

『检查规则』用来设置『接入准入策略』关联的『检查规则』。实现将用户和『检查规则』相关联。

点击编辑规则列表，打开『规则编辑列表』选择需要关联的检查规则。

页面如下所示：



配置完成，点击确定，保存设置。

点击保存，即可完成并保存设置。

点击提交并继续添加，即保存的当前基本规则的设置，同时不返回『端点安全策略』页面，可继续添加规则。

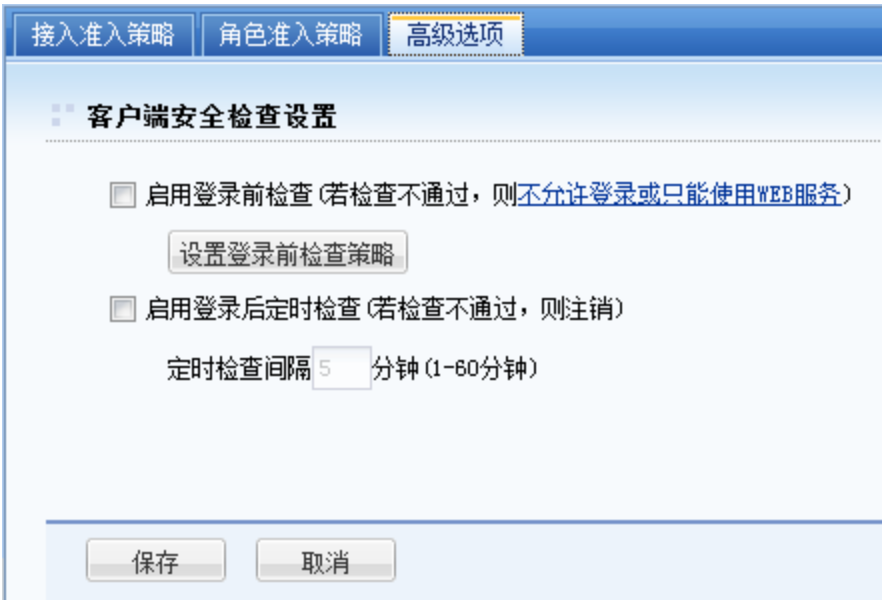
点击取消，取消设置。

『选择关联角色』的前提需要已建立好相应的角色，如何 建立角色，请参考 4.6 章节。

『高级设置』用于客户端安全检测设置。

『客户端安全检测设置』可以设置[启用登录前检查]和[启用登录后定时检查]。

页面如下所示：



[启用登录前检查(若检查不通过，则不允许登录或只能使用 WEB 应用资源)]设置用户成功登录 VDI 前通过『检查规则』对客户端进行检查，检查通过，允许登录 VDI；检查不通过，则不允许登录或只能使用 WEB 应用资源。

点击设置登录前检查策略，打开【编辑规则】窗口，点击编辑规则列表，勾选需要检查的检查规则。

配置完成，点击确定，保存设置。

注意：此功能是全局启用，开启后所有用户都将进行安全检测。

[启用登录后定时检查（若检查不通过，则注销）]，在『定时检查间隔』后面方框填写检查的时间间隔，单位为分钟。然后点击保存，再点击配置生效，保存配置并生效。

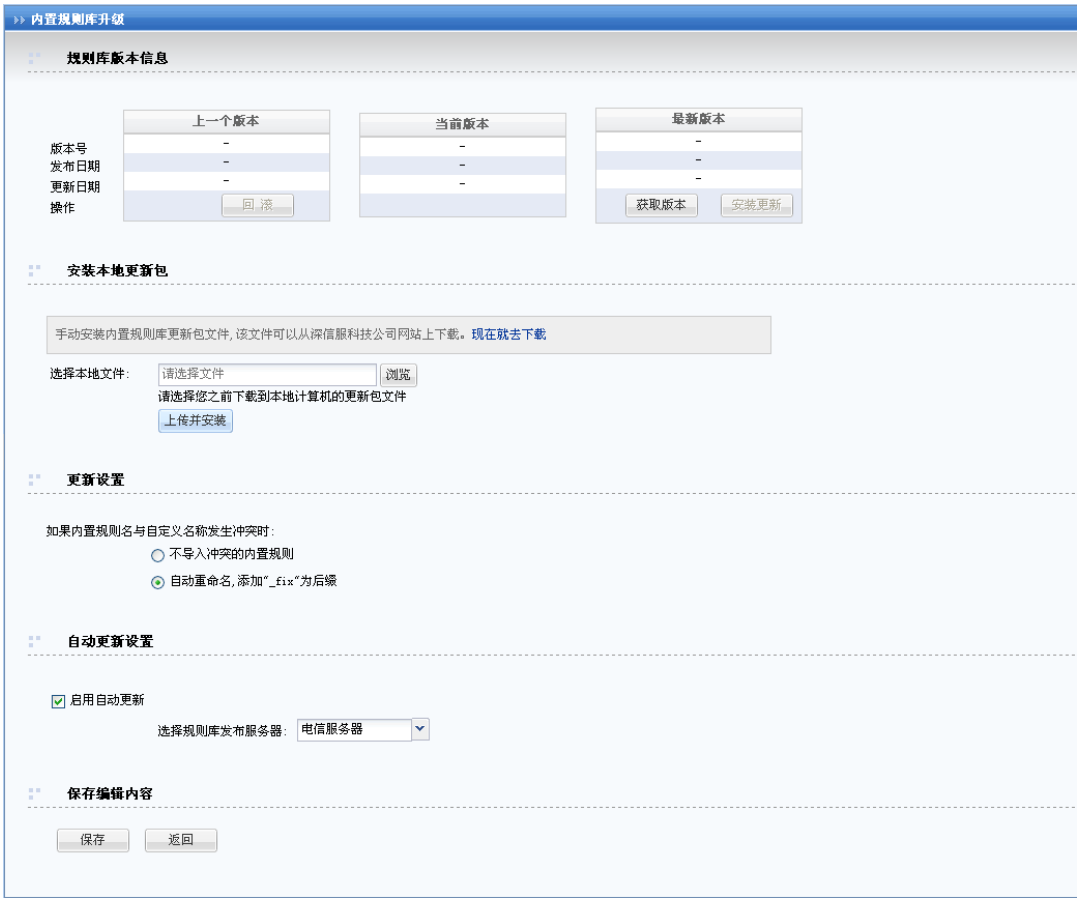
注意：若一个用户同时关联了『接入准入策略』和『角色准入策略』两个策略，当用户接入时，会先检查『接入准入策略』，如果检测不通过，则注销用户；如果『接入准入策略』通过了，但是『角色准入策略』没有通过，则将资源放入『未获授权资源列表』。

4.9.3. 内置规则库升级

WEBUI 路径：『VDI 设置』→『端点安全』→『内置规则库升级』。

除了可以自定义规则和策略外，还可以使用深信服提供的规则库。深信服内置的规则库会定期的更新，用户可以从内置库中找到比较常用的规则，方便用户的使用。

页面所下所示：



在『规则库版本信息』中点击获取版本即可从深信服的内置规则库更新服务器上获取到最新的内置策略库版本信息，点击安装更新即可将内置规则库更新为最新版本，点击回滚可将内置规则库回滚至此台设备之前使用的内置策略库。

『安装本地更新包』提供给用户手动下载更新内置规则库，点击现在就去下载即可访问到深信服内置规则库下载页面，下载需要的内置规则库后，点击浏览找到该规则库，再点击上传并安装即可。

『更新设置』提供了两种内置规则的名称与自定义规则冲突时的处理方法。

勾选[不导入内置规则]，则当内置规则和自定义规则名称冲突时，不会导入该条内置

规则。

勾选[自动重命名，添加“_fix”为后缀]，则当内置规则和自定义规则名称冲突时，会自动修改内置规则的名称，将内置规则添加“_fix”的后缀。

[启用自动更新]将自动从深信服的内置规则库更新服务器上去更新最新的内置规则库。通过下拉框指定从[电信服务器]或[网通服务器]上去更新。

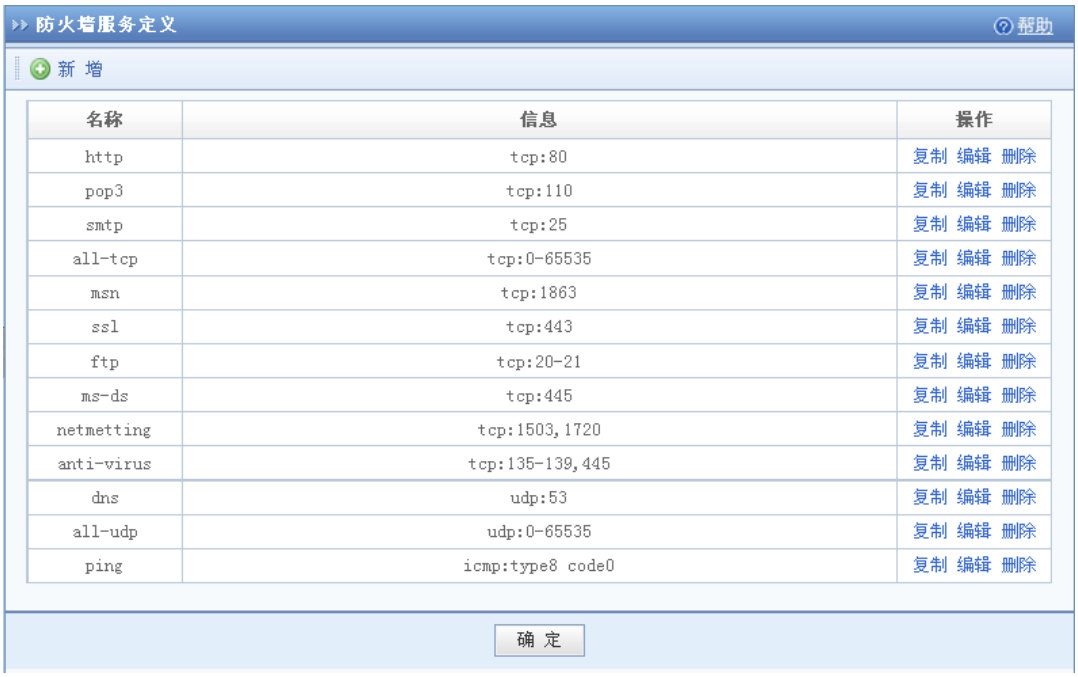
点击保存，保存设置。

第5章 防火墙设置

SANGFOR VDC 硬件网关集成了高性能的企业级状态检测防火墙，能有效保护内部网络免受来自包括 Internet、客户端连接的其它局域网等多方面的攻击。同时，内置的防 DOS 攻击功能，不仅可以有效防范来自外部网络的 DOS 攻击，对于内网计算机发起的 DOS 攻击，SANGFOR VDC 硬件网关也可以进行防御。

5.1. 服务定义

通过网络运行的软件和通信程序使用不同的传输协议和端口，在设定针对这些数据的防火墙规则之前需要先定义其传输协议和端口，页面如下：



例如：需要在 SANGFOR VDC 硬件网关上对 SQL SERVER 服务数据的传输设置规则，首先需要对 SQL SERVER 服务所使用的协议和端口进行定义，点击新增，出现【防火墙信息编辑】对话框，页面如下：

『服务名称』可自定义（本例中可设置为：SQL）。

『服务定义』选择定义服务的协议类型，本例选择 TCP。

『目标端口』填写提供服务的端口号，本例填写 1433。

点确定保存即可完成对 SQL SERVER 服务的定义。

5.2. IP 组定义

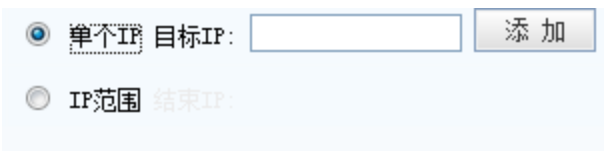
在设定针对特定 IP 的防火墙规则之前需要先定义这些 IP，页面如下：

例如：需要在 SANGFOR VDC 硬件网关上对源 IP 地址为 192.168.1.0/24 数据的传输设置规则，首先需要定义这个 IP 段，点击新增，出现『防火墙 IP 组编辑』对话框，页面如下：

『IP 组名称』可自定义。

『IP 范围』IP 地址范围，可填单个 IP 或 IP 段，本例填写 192.168.1.1-192.168.1.254。点确定保存即可完成对 IP 段的定义。

若选择为单个 IP，则只需要填写一个目标 IP 地址，如下图：

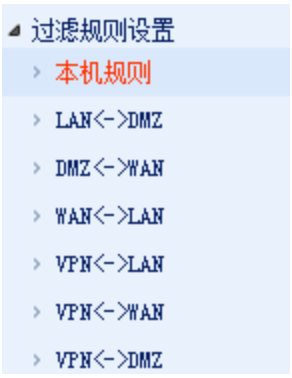


5.3. 过滤规则设置

SANGFOR VDC 硬件网关防火墙采用状态检测包过滤技术，可在多个数据传输方向

上结合时间计划实现基于协议类型、源 IP、目的 IP 的数据包过滤。

可设置包括了本机规则和十二个方向的规则设置。如下图：



所有的 VPN 数据都会经由 VPN 接口传输（例如：本端设备 LAN 接口下的计算机与 VPN 对端计算机的数据通信是经由设备 LAN 接口与 VPN 接口传输），因此防火墙 的过滤规则可以对 VPN 数据进行控制。

『本机规则』用于设置对本机的防火墙策略。

点击[启用]或[禁用]来开启或禁用本条策略。

点确定保存即可完成对本机策略的设置。

『LAN<->DMZ』用于设置 VDC 设备的 LAN 接口与 DMZ 接口之间双向数据传输的防火墙过滤规则。

『DMZ<->WAN』用于设置 VDC 设备的 DMZ 接口与 WAN 接口之间双向数据传输的防火墙过滤规则。

『WAN<->LAN』用于设置 VDC 设备的 WAN 接口与 LAN 接口之间双向数据传输的防火墙过滤规则。

『VPN<->LAN』用于设置 VDC 设备的 VPN 接口与 LAN 接口之间双向数据传输的防火墙过滤规则。

『VPN<->WAN』用于设置 VDC 设备的 VPN 接口与 WAN 接口之间双向数据传输的防火墙过滤规则（如果 VPN 连接对端在『隧道间路由设置』中设置了以本端作为『目的路由用户』并启用『通过目的路由用户上网』，则在本端可通过设置 VPN<->WAN 的过滤规则实现对分支上网数据的控制）。

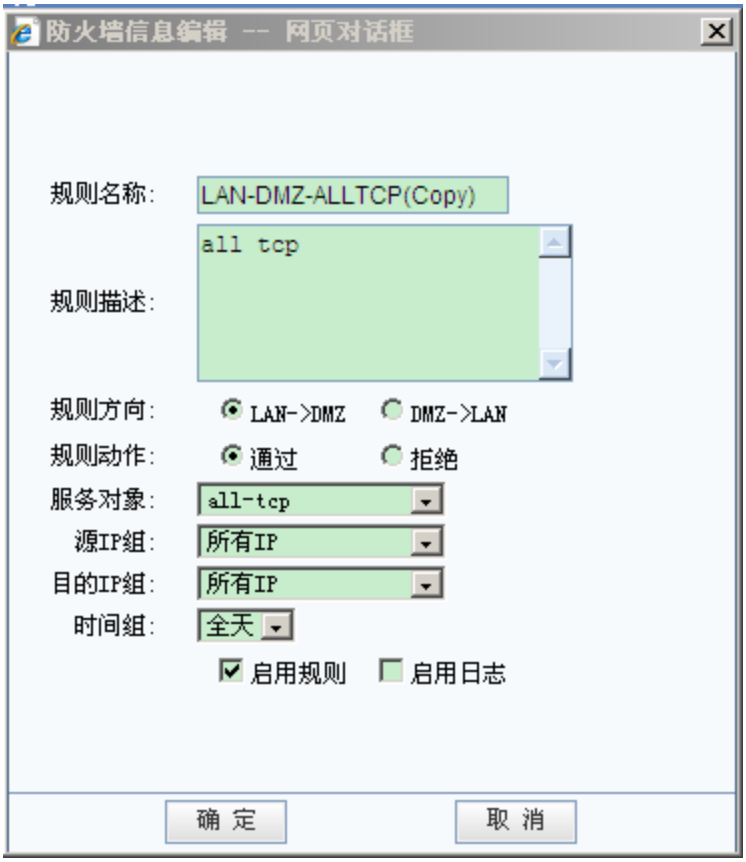
『VPN<->DMZ』用于设置 VDC 设备的 VPN 接口与 DMZ 接口之间双向数据传输的防火墙过滤规则。

下面以 LAN<->DMZ、VPN<->LAN 为例介绍过滤规则设置的一般步骤：

1、LAN<->DMZ

用于设置 LAN 口与 DMZ 口之间数据传输的防火墙过滤规则，可根据实际环境设置放行某类服务数据或拒绝某类服务数据。例如要使 LAN 与 DMZ 口之间完全互通并且能够使用 PING 命令进行测试，则需要在两个方向上开放所有的 TCP、UDP 以及 ICMP 过滤规则。页面如下：

设置规则时需要注意数据的方向和动作，页面如下：



『规则名称』自定义规则名称。

『规则方向』设置此规则对哪个方向的数据生效。

『规则动作』设置数据匹配此规则后的执行动作。

『服务对象』设置规则要匹配的服务类型。

『源 IP 组』设置规则要匹配的源 IP 地址。

『目的 IP 组』设置规则要匹配的目的 IP 地址。

『时间组』设置规则生效的时间。

勾[启用规则]选项，则此规则设置完成后立即生效。

勾选[启用日志]选项，则所有匹配此规则的数据包经过设备时日志系统都将记录日志，一般情况下请不要启用，以免系统产生大量日志。

2、VPN<->LAN

此界面用于设置 VPN 接口与 LAN 接口之间数据传输的防火墙过滤规则，默认规则已放行了双向的所有 TCP、UDP、ICMP 数据，页面如下：

5.4. NAT 设置

NAT 设置包括『代理上网设置』、『端口映射设置』、『IP MAC 绑定设置』、『HTTP 端口设置』、『URL 组设置』、『外部服务组设置』、『用户上网权限设置』等内容。

5.4.1. 代理上网设置

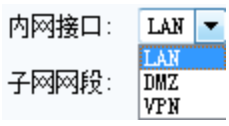
『代理上网设置』用于设置防火墙代理局域网上网的规则，SANGFOR VDC 硬件网关不仅有基本的 NAT 代理上网功能，还可通过与过滤规则进行配合对内网的上网服务进行控制。

WEBUI 路径：『防火墙设置』→『NAT 设置』→『代理上网设置』。如下图：

设备缺省设置中不包含代理信息，需要手动添加，点击新增，弹出【代理网段配置编辑】对话框，页面如下：

[名称]自定义即可。

[内网接口]需要代理上网的用户在设备的哪个接口中，包括 LAN，DMZ，VPN。如下图：



[子网网段]要代理上网的网段。

[子网掩码]代理上网网段的掩码。

勾选[启用]，即启用该规则，启用后，防火墙将自动放通相应的过滤规则。

5.4.2. 端口映射设置

『端口映射设置』用于设置防火墙的 DNAT 规则，如果局域网内的服务器需要向外网提供服务，则需要添加『端口映射设置』。

WEBUI 路径：『防火墙设置』→『NAT 设置』→『端口映射设置』。界面如下图所示：

5.4.2.1. 案例学习

内网有一台 IP 为 192.168.10.20 的电脑要对外网提供 Web 服务，所使用的端口为 80，需要通过端口映射将该服务器 80 端口发布至公网，则设置步骤如下：

1、在『端口映射设置』中『新增』一条映射规则。页面如下：

点击确定后规则生效，则外网可通过端口映射功能访问到内网提供的 Web 服务。

注意：通过 SANGFOR VDC 硬件设备设置端口映射向外网提供服务的内网服务器，必须是以 VDC 设备设备作为 NAT 代理上网（网关指向 VDC 设备或上网路由最终指向 VDC 设备），否则端口映射将无法生效。

5.4.3. IP MAC 绑定设置

SANGFOR VDC 系列产品提供了“IP/MAC 绑定”功能，通过此功能可以很方便地得到内网某个 IP 地址所对应的 MAC 地址并将它们绑定在一起，当局域网内部有未知设备接入时，由于在 IP/MAC 绑定表中没有它的记录，未知设备将无法通过 VDC 网关上网。当某个 IP 所对应的 MAC 地址与记录不符时，VDC 网关也将拒绝此 IP 的上网请求，因此 IP/MAC 绑定还可用于限制内部电脑 IP 被人为改动。

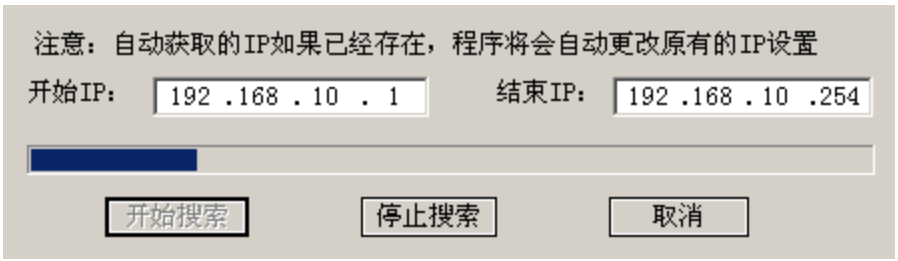
WEBUI 路径：『防火墙设置』→『NAT 设置』→『IP MAC 绑定设置』。

界面如下图所示：

勾选[启用 IP MAC 绑定]即启用 IP-MAC 绑定功能。

点击新增，手动添加 IP 和 MAC 的对应关系。也可以点击自动获取来自动获取 IP 所对应的 MAC 信息。

点击自动搜索，设置搜索范围，系统将自动在所设置的 IP 范围内搜索存在的计算机的 IP/MAC 信息。



『IP 不在表中的行为』可选为[拒绝]或[通过]，用于设置不匹配 IP/MAC 记录后的操作。

[拒绝]即对不在 IP MAC 列表内的计算机以及列表内 IP MAC 不匹配的计算机禁止上网，对 IP MAC 匹配的计算机依旧允许其上网。

[通过]即对不匹配 IP MAC 记录的计算机以及不在 IP MAC 列表内的计算机允许其上网，在 IP MAC 列表内的计算机如果 IP MAC 匹配正确则允许上网，匹配不正确依旧不允许上网。

IP/MAC 绑定功能，不支持内网有三层设备的环境。

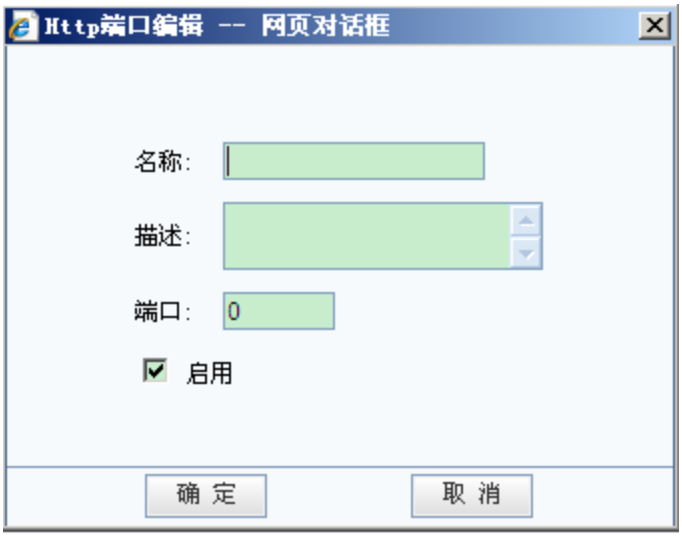
5.4.4. HTTP 端口设置

『HTTP 端口设置』用于定义 HTTP 服务的端口，默认设置为 80。这里定义 HTTP 端口为 80 后，当启用[上网权限/启用 URL]记录功能时，VDC 设备网关会记录通过 80 端口访问的 URL 信息并可对通过 80 端口发出 URL 信息进行过滤，如果需要记录/过滤通过其它端口访问的 URL 信息，则需将相应的端口添加到『HTTP 端口设置』中。

WEBUI 路径：『防火墙设置』→『NAT 设置』→『HTTP 端口设置』。

界面如下图所示：

点击新增，设置『名称』、『描述』、『端口』，勾选[启用]，完成设置。



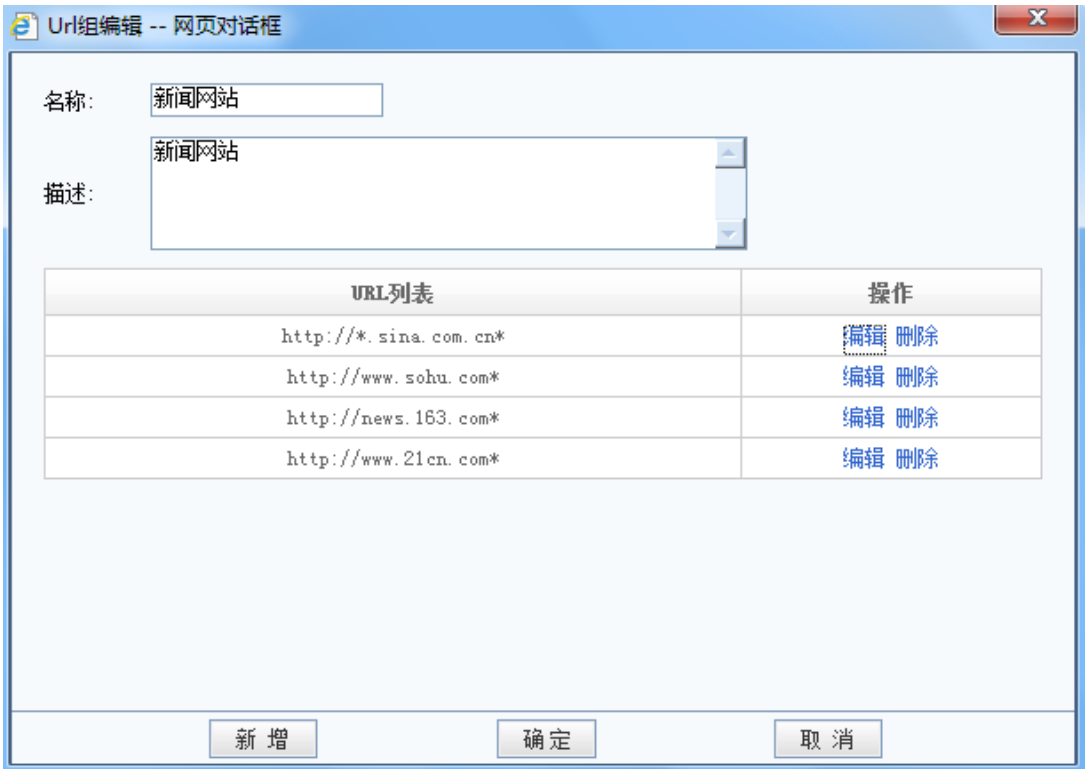
5.4.5. URL 组设置

VDC 设备网关的企业级状态检测防火墙具有“网页地址过滤”功能，可与防火墙配合对局域网用户上网进行管理，使用该功能之前需要先在『URL 组设置』中添加所需的 URL 信息。

WEBUI 路径：『防火墙设置』→『NAT 设置』→『URL 组设置』。

界面如下图所示：

点击上图中新增按钮，显示『URL 组编辑』对话框，设置 URL 组『名称』、描述。在点击下图中新增，将 URL 信息添加到『URL 列表』中（第一个字段支持使用*号匹配），如有需要可添加多个 URL，点确定后完成设置，页面如下：



5.4.6. 外部服务组设置

默认情况下，内网用户可以访问外网的所有服务，如需在『上网权限设置』中设置内网用户访问外网服务的权限，则需先在『外部服务组设置』中定义相应的服务。

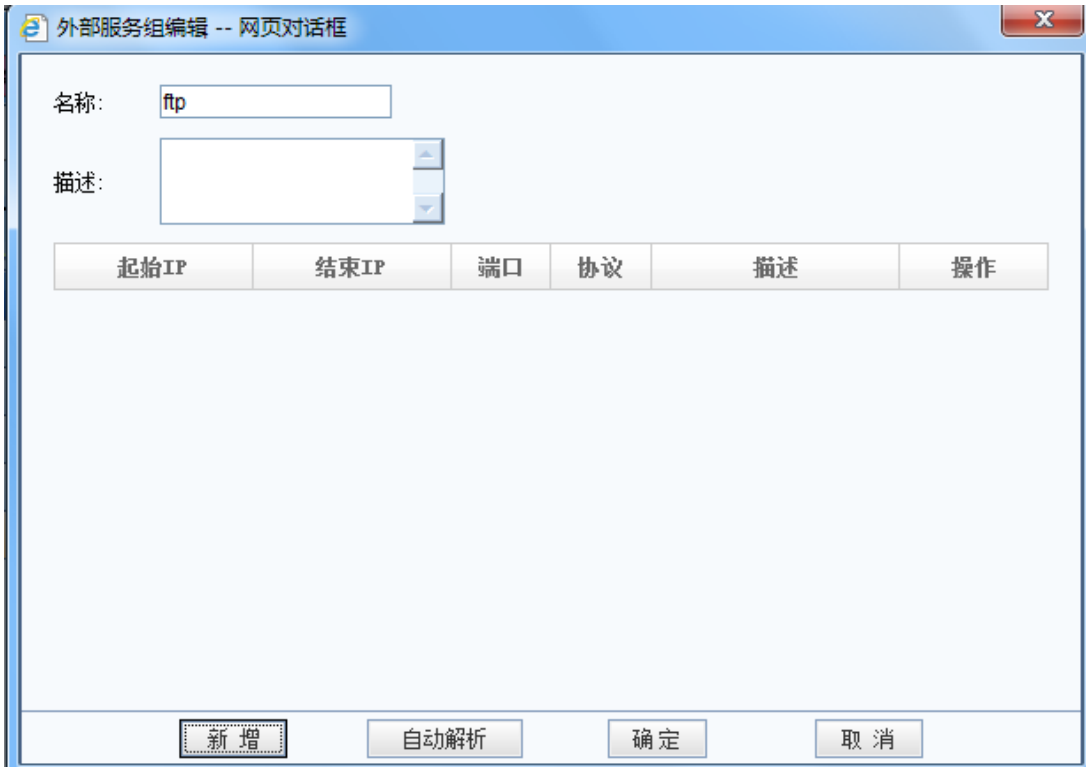
WEBUI 路径：『防火墙设置』→『NAT 设置』→『外部服务组设置』。

界面如下图所示：

默认配置了 POP3、SMTP、WEB、DNS 四类服务，可自定义其他服务。

例如：要添加 Internet 上 IP 为 202.96.137.75 的服务器提供的 FTP 服务（具体端口号根据软件所使用端口而定），设置方法如下：

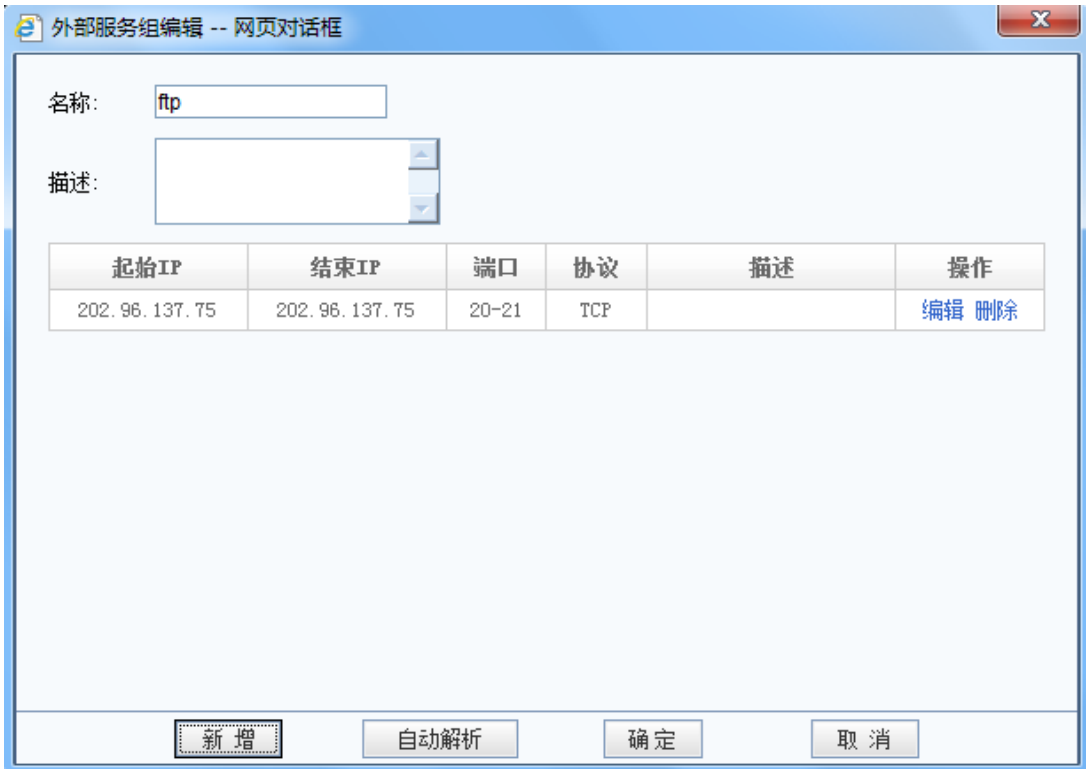
点击新增，显示『外部服务组编辑』对话框，页面如下：



再点击新增，设置外网服务器的『起始 IP』、『终止 IP』、『端口号』、『描述』，页面如下：

也可以点击自动解析按钮出现以下对话框，填入对应的域名，可以自动解析域名对应的 IP，方便定义外网服务。页面如下：

点击确定，保存配置，如下图：



5.4.7. 用户上网权限设置

『用户上网权限设置』是防火墙中用于对局域网用户访问外网的权限进行控制而采用的最常用的方法，虽然通过防火墙的过滤规则也可实现，但这两者仍有区别。『过滤规则』是基于对某些 IP 地址和端口的访问控制来实现上网服务的控制，它更注重的是整个网络的安全性。而在控制内网用户上网时，使用『用户上网权限设置』进行控制时会更为方便。

WEBUI 路径：『防火墙设置』→『NAT 设置』→『用户上网权限设置』。

界面如下图所示：

要启用“URL 过滤”及『访问记录』功能，必须勾选[启用 URL]。

点击新增出现【上网权限编辑】对话框，

在『IP 组』选项卡下点击新增，即可在对话框中输入这条规则所要匹配的内网 IP 范围，页面如下：

点击服务组选项卡，则可设定该内网 IP 范围内，可以访问外网的哪些服务，页面如下：

在此对当前 IP 组能够访问的外网服务进行设置，默认设置是[缺省允许]，此时局域网用户可访问外网的所有服务。相应的服务请在『外部服务组设置』中添加。

点击『URL 组』选项卡，如下图：

在此可以对当前 IP 组访问的 URL 地址进行设置，默认设置是『缺省允许』，如果要

对某个 URL 组进行拦截只需要把它右移并勾选拒绝即可，相应 URL 信息请在『URL 组设置』中添加。

防火墙规则匹配均按照从上往下匹配的原则。配置规则的时候，请注意排序。

5.5. 访问监控

5.5.1. 流量排名

通过『流量排名』可以直观地查看当前局域网中用户对带宽的使用情况，可分别查看上行和下行流量。

WEBUI 路径：『防火墙设置』→『访问监控』→『流量排名』。

界面如下图所示：

5.5.2. 访问记录

『访问记录』用于查看当前局域网用户的 URL 访问记录，点击刷新状态可实时刷新访问记录。

WEBUI 路径：『防火墙设置』→『访问监控』→『访问记录』。

界面如下图所示：

注意：必须在『用户上网权限设置』中勾选『启用 URL』，此处才能看到 URL 访问记录。

5.6. 防 DOS 攻击

防火墙不仅肩负着阻隔 Internet 上的用户对局域网非法攻击的任务，很多时候由于局域网内有电脑中毒，会向网关发送大量的数据包，这样有可能会造成带宽阻塞或者网关死机。SANGFOR VDC 设备内部集成了『防 DOS 攻击』功能，可以监测单位时间内某个 IP 向网关发送了多少数据量，当超过一定值时则 VDC 设备会认为受到此 IP 的 DOS 攻击，并会阻断此 IP 一段时间从而保护自己。页面如下：

勾选[启用防 DOS 攻击]即开启防 DOS 攻击功能。

在『内网网段列表』中添加局域网所包含的网段，当这里为空的时候即表示不检查 IP 地址。当添加了内网网段后，当源 IP 不属于『内网网段列表』所列网段范围之内，则该数据包会被直接丢弃。属于『内网网段列表』范围时，则会进行下面防 DOS 攻击各项设置的计算和探测，以进行相应的处理。

同理，『内网路由器列表』的功能和『内网网段列表』功能类似。

在『排除地址列表』中添加局域网所包含的 IP 地址，当这里为空的时候即表示检查所有 IP 地址。当添加了内网 IP 后，来自这个 IP 地址的攻击不会被防御。

其它选项可根据情况来进行相应设置，包括『最大 TCP 连接数』，『最大 SYN 包数』及『防 DOS 攻击的封锁时间』等。

5.7. QOS 级别设置

QoS(Quality of Service，服务质量保证)在网络带宽不足的情况下，通过 QOS 设定来保证一些重要的服务能获得充足的网络带宽。可以设定各优先级能够得到的带宽比例，在网络繁忙时将按照设定的比例来分配网络带宽，保证整个出口线路上，通过防火墙的重要服务能够顺畅进行。

『QoS 优先级别设置』可以设定四个级别占用的带宽比例，以百分比来表示。

『启用 QoS 功能』是整个防火墙 QoS 功能的开关，勾选即启用了防火墙的 QoS 功能。

5.8. QOS 上传规则设置

QoS 上传规则设置是用来把数据业务进行分类，根据 QoS 规则设置所选定的数据投递优先级进行投递，以保证重要数据的及时传输。

设备内置了一项缺省服务定义，只需点击编辑按钮，即可设置默认服务的优先等级信息。

点击新增按钮，会出现以下【新增 QoS 规则】对话框：

『服务名称』和『描述』可根据喜好填写。

『服务优先级』用于设置该 QoS 规则应用的“优先级”，除了前面『QoS 等级设置』定义的四个等级外，还有一个“特权级”，特权级别可以占用所有带宽。

勾选[启用该服务]即可激活这条 QoS 上传规则。

『IP 地址』用于设置 QoS 规则应用的源及目标 IP，可以设定为“所有 IP 地址”或“指定 IP 地址”。

『协议』用于设置 QoS 规则所对应的服务提供的端口及协议等。

5.9. QOS 下载规则设置

QoS 下载规则设置是用来把数据业务进行分类，根据 QoS 规则设置所设定的不同服务优先级进行投递，以保证重要数据的及时传输。

和 QoS 上传规则相类似，点击新增按钮出现如下对话框，以下仅举一例子说明：

以上规则保证了内网从公网 HTTP 服务器 80 端口的下载通讯设定 QoS 级别为特权级别。

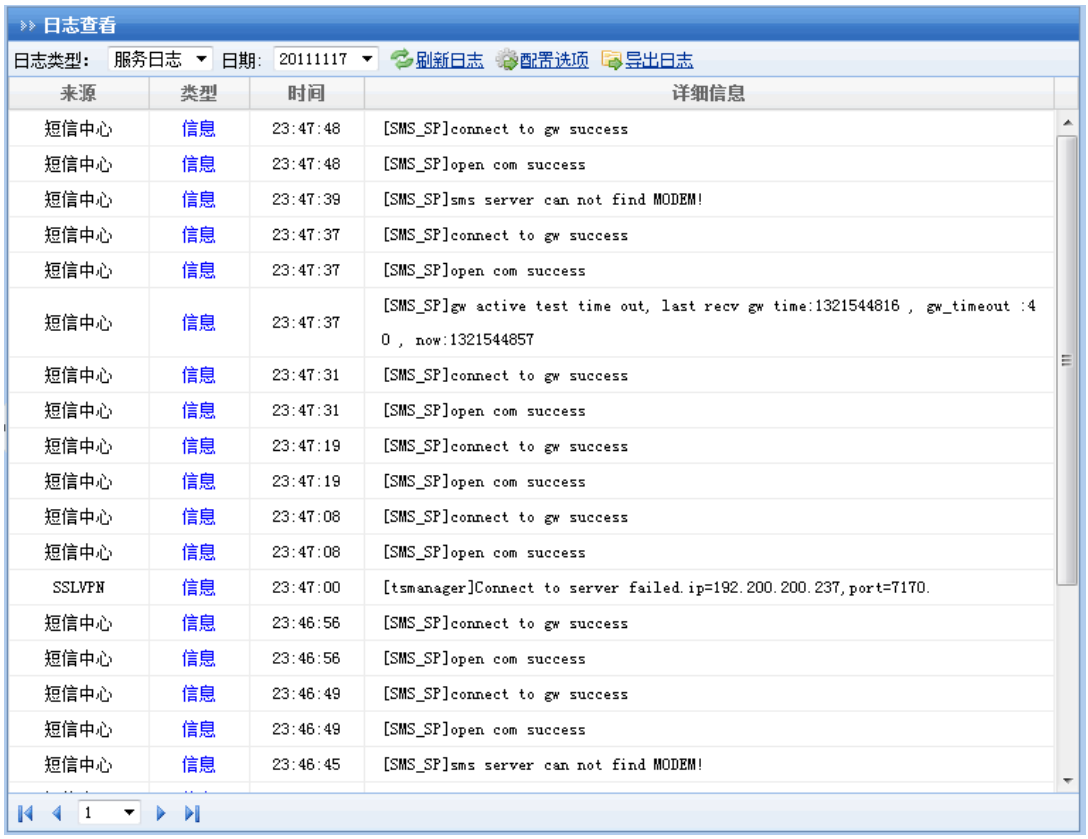
第6章 系统维护

『系统维护』包括『日志查看』、『配置备份/恢复』、『重启/重启服务/关机』和『系统更新』四部分。

6.1. 日志查看

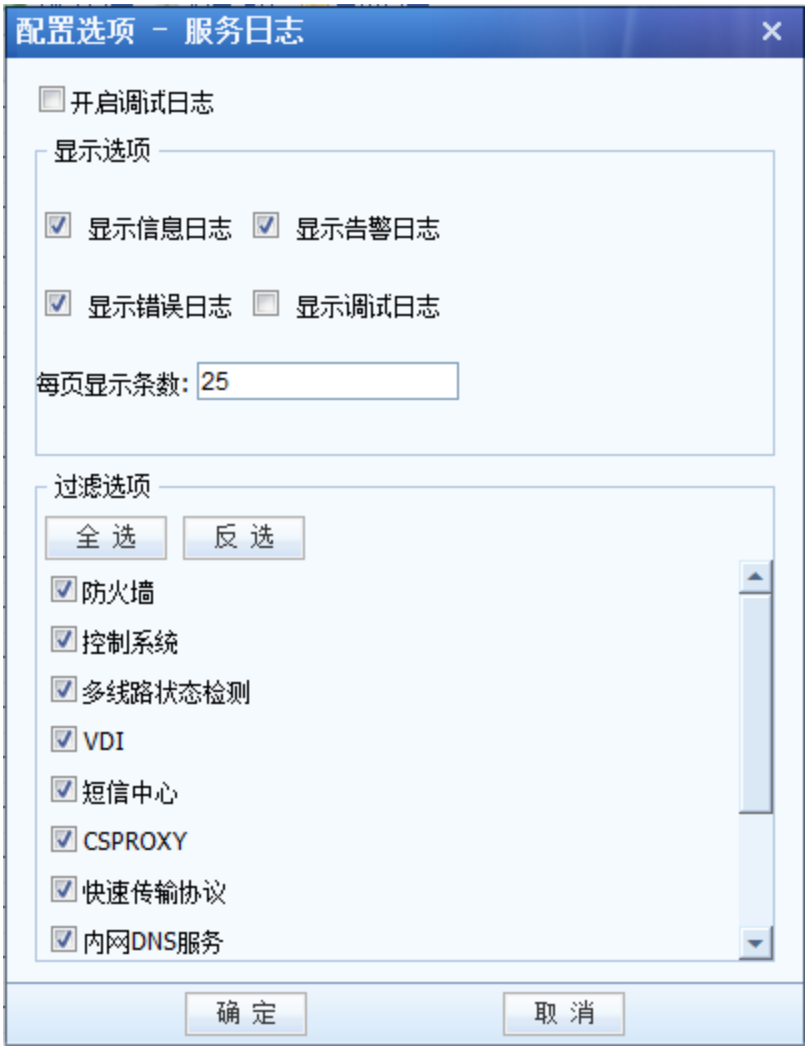
用于查看设备的运行日志及错误提示。运行日志包括了两种类型，一种为服务日志，另一种为管理日志。服务日志可以查看当前设备各种服务运行的信息。选择要查看的日期，会显示相应时间下的日志记录。

WEBUI 路径：『系统维护』→『日志查看』。界面显示如下：

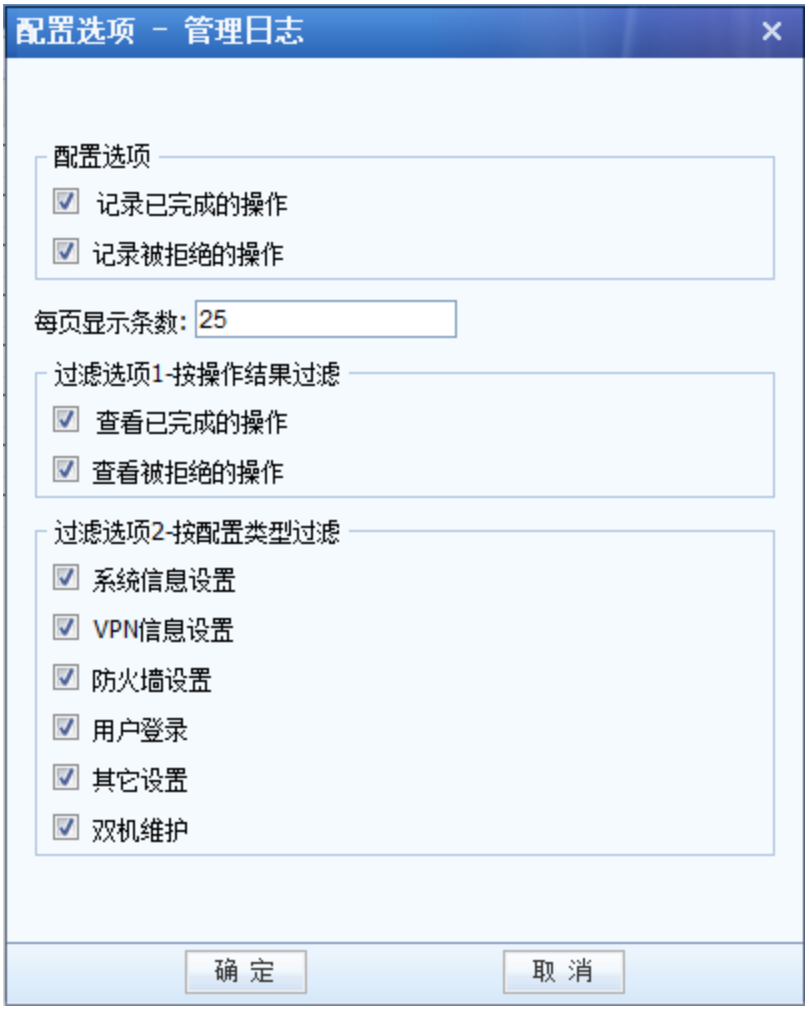


『日志类型』中，默认显示的是[服务日志]，也可以选择[管理日志]，[管理日志]主要用来查看当前设备管理员对设备进行的操作日志信息，如下图：

在[服务日志]下点配置选项，可以设置指定查看的系统日志范围。页面如下：



在[管理日志]下点配置选项，可以设置指定查看的管理日志范围。页面如下：



注意：VDC 设备最多保留 7 天的日志，超出 7 天的日志将被清空。

6.2. 配置备份/恢复

『配置备份/恢复』用于备份、恢复 VDC 设备的配置。

WEBUI 路径：『系统维护』→『配置备份/恢复』。

界面显示如下：

『全局配置备份』标签页，设置备份和还原设备的所有配置。

通过设备备份 VDI 的全局配置时，会备份 VDI 的序列号，所以，在配置还原 VDI 的全局配置前，注意备份需要还原设备的序列号。

点击下载当前配置，可将当前的配置备份到本地 PC 上，以便以后恢复，下载下来的文件格式为.bcf。

点击开始还原，可将以前备份在本地 PC 上的配置导入设备。

勾选[连续一段时间内没有执行配置备份,则登录控制台时提醒]并设置好『时间间隔』后，系统会以设置的时间为间隔在用户登录控制界面时提醒用户进行备份。

『VDI 配置备份』标签页，设置备份和还原 VDI 的所有配置。

界面显示如下：

点击『下载当前配置』，可将 VDI 模块中的配置下载下来保存在本地 PC 当中。

注意：这里的下载配置只能下载 VDI 模块的配置，此配置不包含系统配置、防火墙等其它模块的配置。

『配置还原』功能用于将 VDI 配置恢复到以前保存的配置。点击浏览，先择以前备份的配置，再点击开始还原即可。

『自动备份配置』：设备自动配置最近 7 天的配置，点击相应该配置文件后的还原配置可以将 VDI 配置恢复到备份时的状态。

6.3. 重启/重启服务/关机

WEBUI 路径：『系统维护』→『重启/重启服务/关机』。

界面显示如下：

关闭设备：将设备安全的关闭。

重启设备：将设备先关闭再重启。

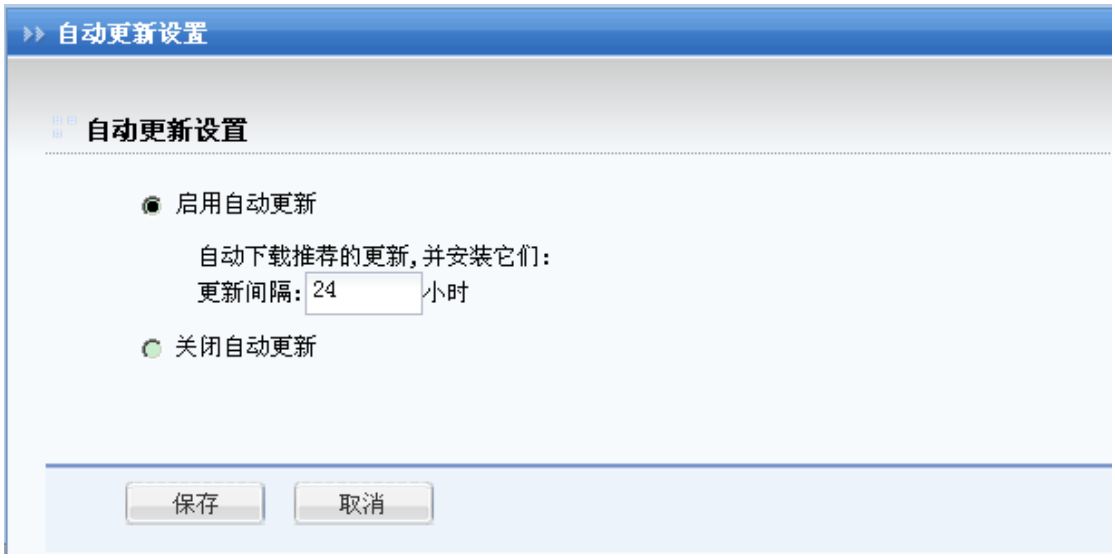
重启所有服务：将当前连接的会话与资源全部释放后，再重启全部服务。

停止 VDI 服务：将 VDI 服务停止。

6.4. 系统更新

选择是否启用自动更新，如果启用，则会自动下载更新，并安装它们。

WEBUI 路径：『系统维护』→『系统更新』。



选择[启用自动更新]，并设置好『更新时间』，设备会每隔设定的时间自动去下载可用更新，并安装它们。

注：此更新不可用于大版本升级。

选择[关闭自动更新]，设备不再去自动下载更新。

点击保存使当前设置生效。

第7章 客户端使用

本部分主要介绍了 VDI 客户端的安装和使用。VDI 的客户端包括普通计算机和 aDesk 瘦客户机。aDesk 瘦客户机的安装和使用方法在单独的用户手册中进行说明，本章重点介绍普通计算机登录使用 VDI。

7.1. 环境要求

1、客户端计算机已经接入网络，网络通信正常，能与 VDC 设备联通。

2、计算机必须安装浏览器。

3、电脑安装 3721、上网助手等工具，可能会影响正常使用，建议先卸载。

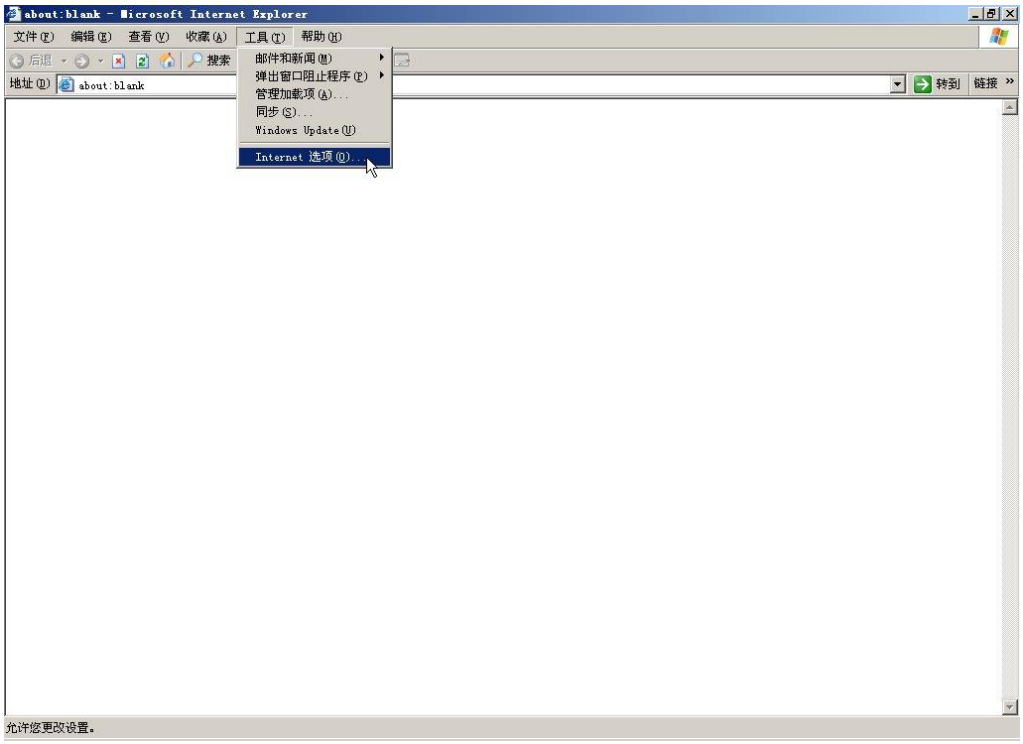
VDI 客户端支持 Windows 操作系统、Linux 操作系统和 Mac OS X 操作系统，支持苹果，安卓等手机接入；支持多种浏览器。

7.2. 典型使用方法举例

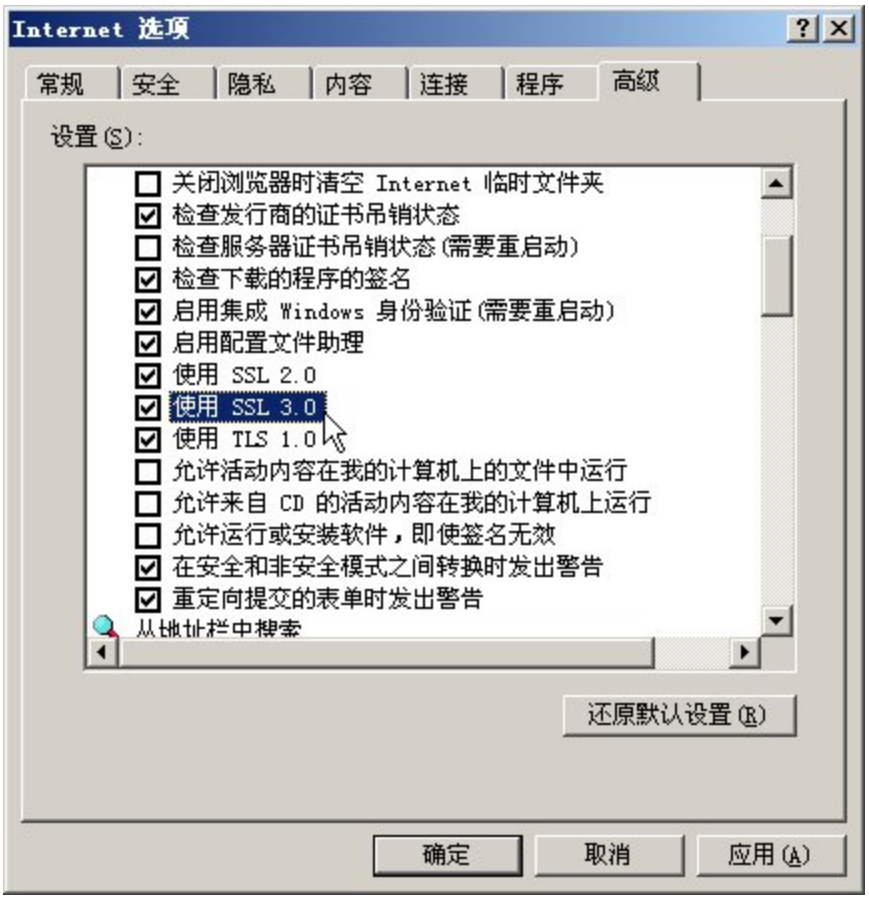
使用 VDI 客户端之前，可能需要对浏览器（例如 IE，以下皆以 IE 作为浏览器来举例）进行必要的设置，步骤如下：

（注：以下所有截图皆以 Windows XP 系统下的 IE 为例，其它操作系统或浏览器，界面可能稍有不同）

打开 IE 中的[工具]－[Internet 选项]，如下图：



打开 Internet 选项中的[高级]选项卡，勾选[使用 SSL2.0]、[使用 SSL3.0]和[使用 TLS1.0]选项，设置如下图：

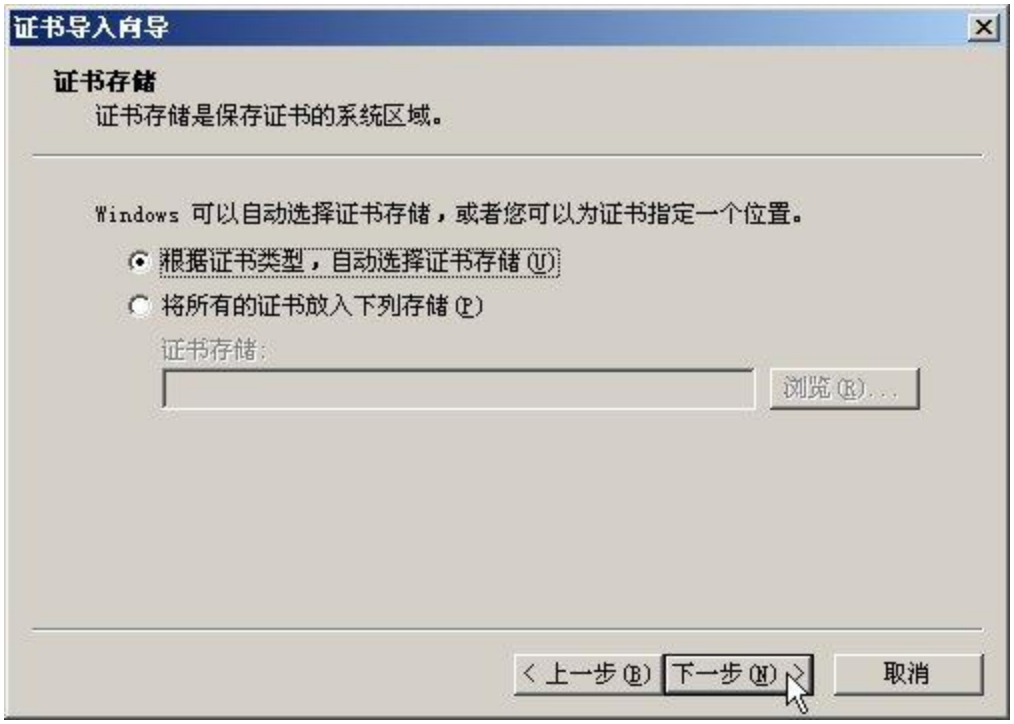


设置好 IE 浏览器之后，直接在 IE 地址栏输入 VDI 客户端的登录页面地址来登录。

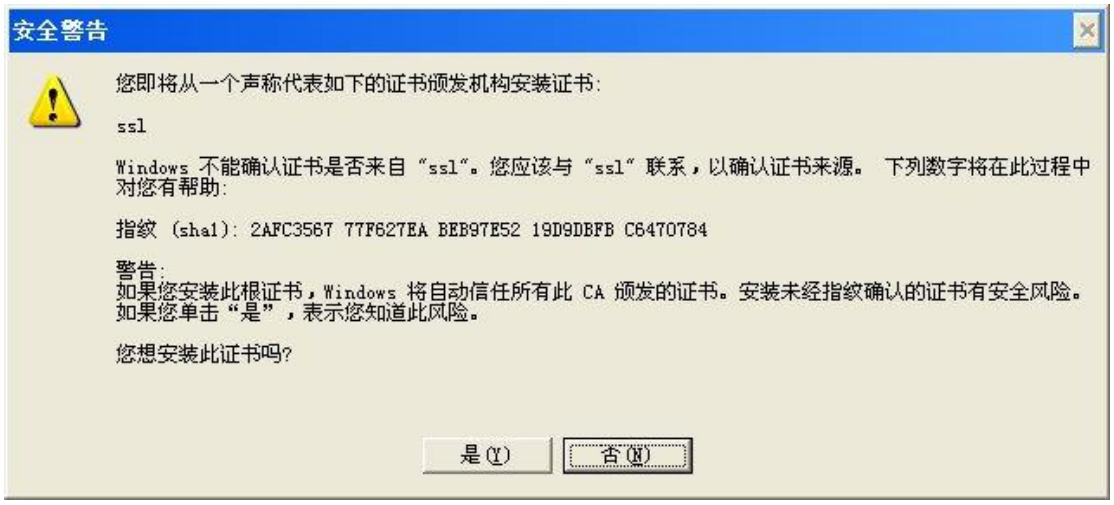
访问 VDI 客户端时，可能会弹[安全警告]，提示需要安装数字证书，如下图所示：

第一次使用时，请点击查看证书按钮，以完成“根证书”的安装。查看证书界面如下：

点击安装证书按钮，然后下一步，选择“证书存储”的位置，如下图：



点下一步，并完成，会出现[安装证书]的警告框如下，选[是]进行安装。

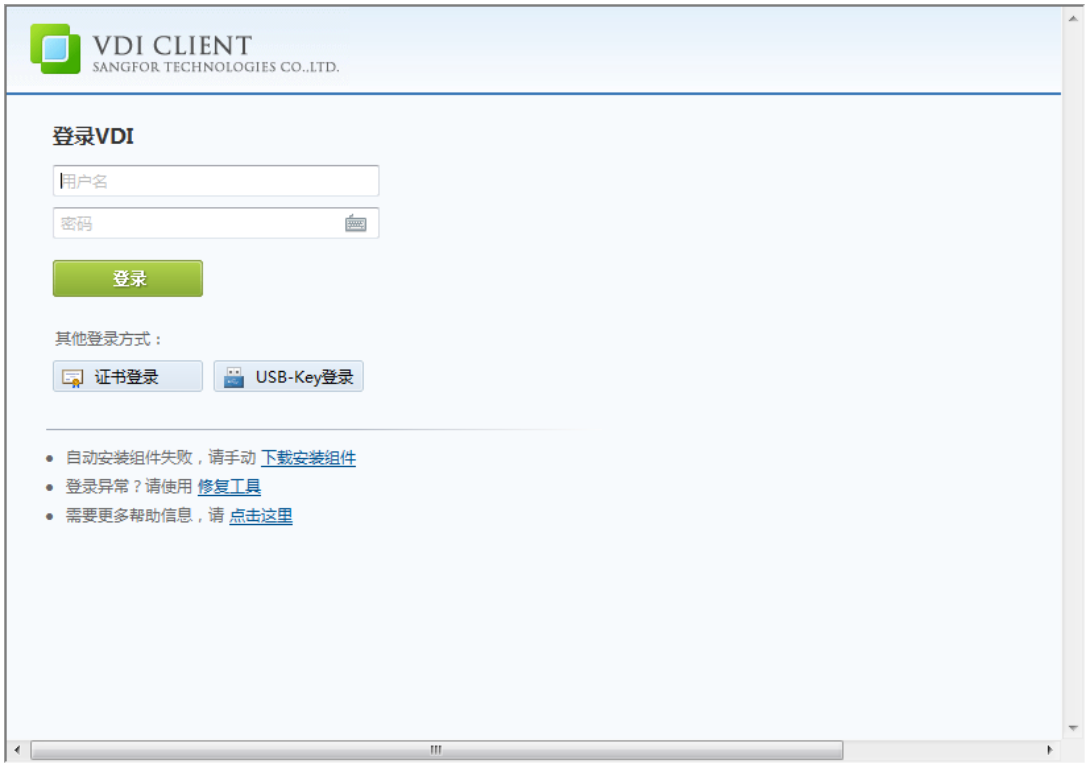


安装完毕后，会有证书[导入成功]的提示。如下图：

[根证书]的安装一般只在第一次登录时需要安装，安装成功后，下次登录在[安全警报]

处，询问是否继续时，直接点[是]即可。

安装好根证书等之后，即进入以下欢迎页面：



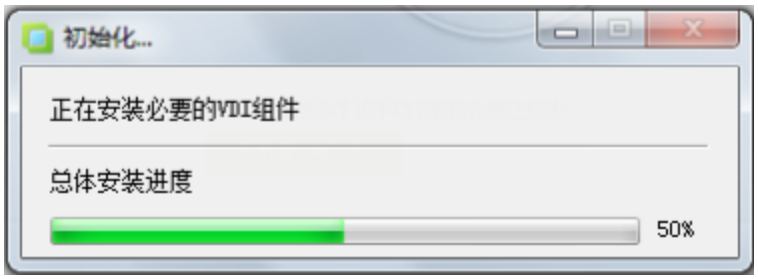
输入用户名密码及校验码后，点击登录，即可登录。

『证书登录』连接用于数字证书认证用户登录（数字证书手动安装在 IE 上的用户）。

『USB-Key 登录』用于使用 USB-Key 认证的用户登录（包括有驱 USB-Key 和无驱 USB-Key）。

登录过程中，会提示安装客户端控件，请允许浏览器自动安装，或者点击【下载客户端控件】按钮手动安装。

安装过程如下：



安装并登录成功后会出现 VDI 资源列表界面如下：

界面会显示该 VDI 用户可用的内网资源列表。点击资源名称即可启动相应的远程应用或者共享桌面。

至此，完成了一次 VDI 用户登陆的过程。

需要退出时，点击右上角的注销按钮，即可安全退出 VDI 客户端。注销之后，用户将不能访问资源。

资源列表上方的设置按钮，可让用户自行修改密码，界面如下：

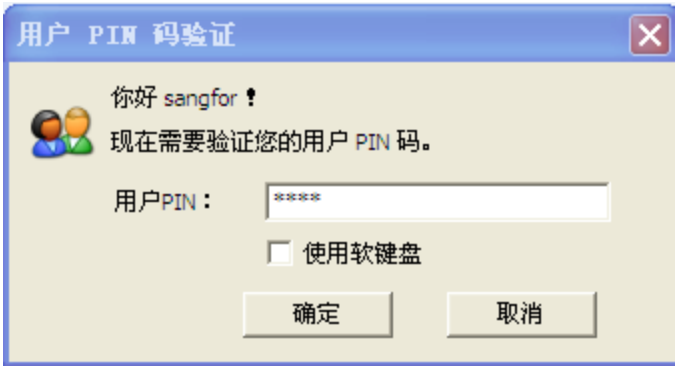
点击 [修改]，如下图所示：

修改后，点击保存即可成功修改用户的登录密码。

「系统设置」下，显示的内容与 VDI 配置有关，请以实际显示的为准。

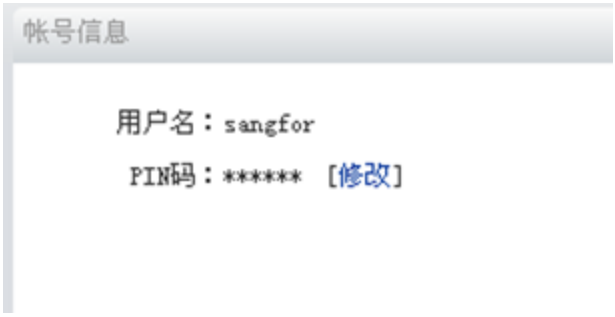
对于使用 USB-KEY 的用户登录 VDI 的过程，和普通用户登录稍有不同。

USB-KEY用户登录时，打开浏览器输入 VDI 登录网址，在登录界面处，插入 USB-Key，点击 USB-KEY 登录即进入 USB-KEY 用户的登录界面，（或前面直接取消修改 PIN 的操作），界面如下：

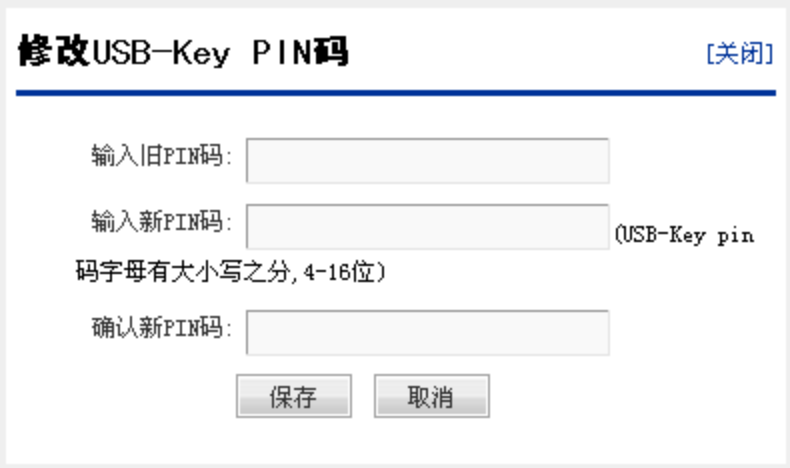


输入用户 USB-Key 的 PIN 码，设备会自动校验客户端信息，校验成功能，即完成 VDI 客户端登录。

USB-Key 用户登录后，点击资源列表上方的设置按钮，可让用户自行修改密码和 USB-Key 的 PIN 码，界面如下：



点击修改，如下图所示：



输入[旧 PIN 码]和[新 PIN 码]，点击保存即修改成功。

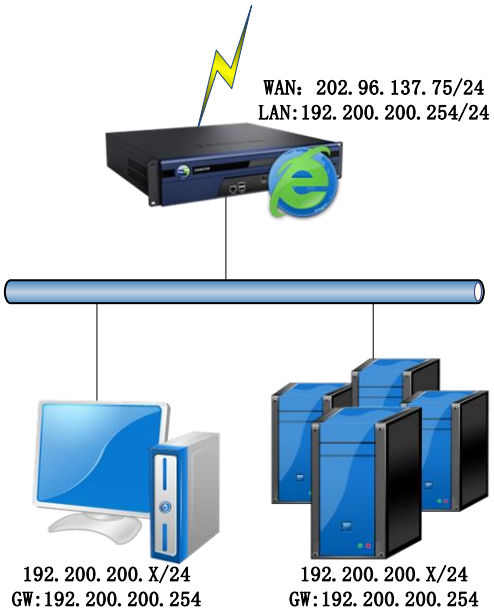
注意：登录 VDI 客户端之后，如果相隔一段时间，没有访问内网资源，或者客户端这边没有任何操作， VDI 客户端会超时，自动注销。超时时间设置请参考 4.8 章节。

第8章 案例集

8.1. 部署配置案例

8.1.1. 网关单线路模式部署

某客户网络拓扑如下图所示，VDC 设备作网关模式部署，代理内网上网，内网一个网段 192.200.200.0/24，外网为以太网类型，从运营商那里分配到的地址为 202.96.137.75。



配置步骤如下：

第一步：进入『系统设置』→『网络配置』→『部署模式』，部署模式选择网关模式，配置好内网接口，界面如下：

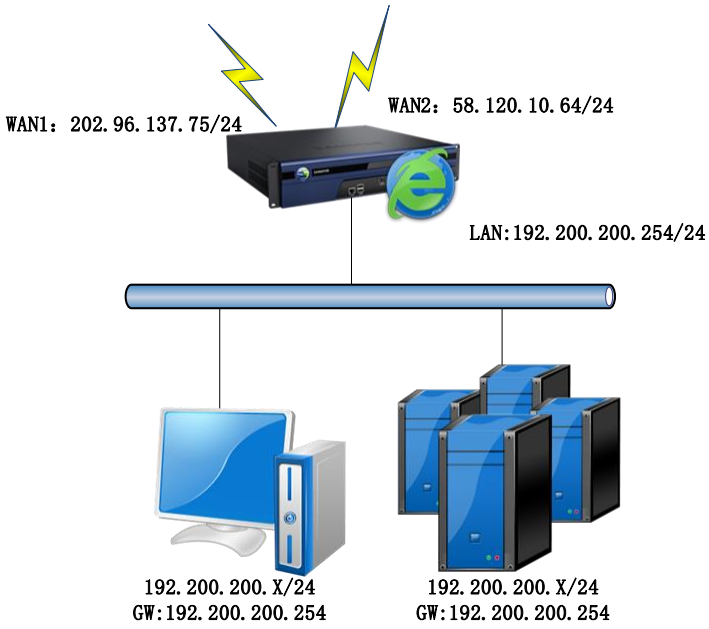
配置好内网接口后，在外网接口配置页面点击相应的线路进行配置，界面如下：

第二步：本案例中 VDC 设备网关模式部署，还需要设备代理内网用户和服务器上网，所以还需要设置代理上网。进入『防火墙设置』→『NAT 设置』→『代理上网设置』，选择新增，配置需要代理上网的内网网段，界面如下：

以上步骤设置完毕，则可以将设备 LAN 口接到交换机，WAN 口接公网链路。部署完毕。

8.1.2. 网关多线路模式部署

某客户网络拓扑如下图所示，外网双线路，一条电信，一条网通，VDC 设备作网关模式部署，代理内网的 PC 和服务器上网，内网一个网段 192.200.200.0/24。客户希望出差在外的人员能够通过最快的链路接入访问。



配置步骤如下：

第一步：进入『系统设置』→『网络配置』→『部署模式』，部署模式选择网关模式，配置好内网接口，界面如下：

配置好内网接口后，在外网接口配置页面点击相应的线路进行配置，界面如下：


编辑线路
启用该线路
线路类型:
以太网
ADSL拨号连接
以太网设置
自动获得IP地址和DNS服务器(DHCP)
使用下面的IP地址和DNS服务器
IP地址:
202.96.137.75
首选DNS:
202.96.134.133
子网掩码:
255.255.255.0
备用DNS:
202.96.128.166
默认网关:
202.96.137.1
多IP绑定
高级设置
保存
取消


编辑线路
启用该线路
线路类型:
以太网
ADSL拨号连接
以太网设置
自动获得IP地址和DNS服务器(DHCP)
使用下面的IP地址和DNS服务器
IP地址:
58.120.10.64
首选DNS:
58.120.10.63
子网掩码:
255.255.255.0
备用DNS:
8.8.8.8
默认网关:
58.120.10.63
多IP绑定
高级设置
保存
取消

第二步：进入『系统设置』→『网络配置』→『多线路』，勾选[启用外网多线路传输]，并且新建好两条线路，界面如下图所示：

勾选[启用多线路]，选择[VDI 用户直接接入本设备]，界面如下图所示：

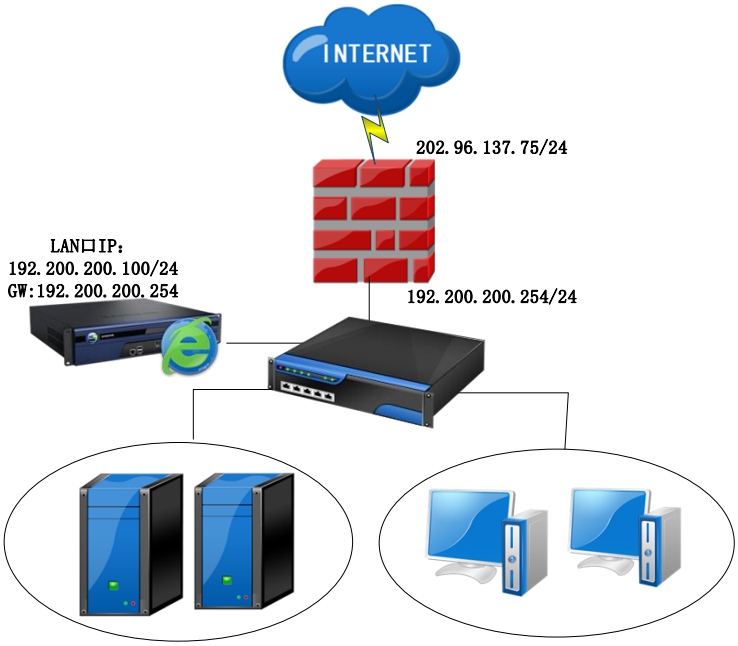
第三步：本案例中 VDC 设备网关模式部署，还需要设备代理内网用户和服务器上网，所以还需要设置代理上网。进入『防火墙设置』→『NAT 设置』→『代理上网设置』，选择新增，配置需要代理上网的内网网段，界面如下：

以上步骤设置完毕，则可以将设备 LAN 口接到交换机，WAN1 口接公网电信链路，WAN2 口接公网网通链路。部署完毕。

仅当 VDC 设备网关多线路直连公网的环境下才需要设置多线路，其他情况下不需要设置多线路。

8.1.3. 单臂单线路模式部署

某客户网络拓扑如下图所示，内网一个网段 192.200.200.0/24，VDC 设备作单臂模式部署，前置防火墙设备通过一条外网接入到 Internet。出差在外的人员希望能够接入访问内网资源。



配置步骤如下：

第一步：进入『系统设置』→『网络配置』→『部署模式』，部署模式选择单臂模式，设置好 LAN 口 IP 地址，掩码和网关。界面如下：

第二步：由于 VDC 设备部署在内网，需要将 VDI 服务对外发布供用户访问，故还需要在前置防火墙设备上做 443 的端口映射给 VDC 设备。VDC 设备建立 VPN 的端口默认

是 TCP 443。各个厂家设置方法有所不同，此处不截图说明。

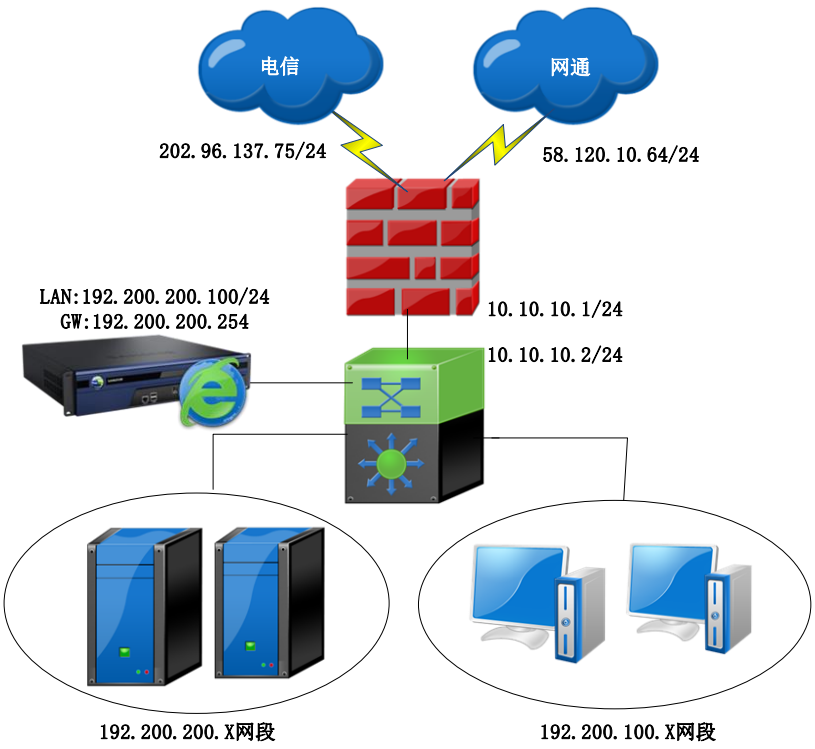
以上步骤设置完毕，则可以将 VDC 设备 LAN 口接到交换机，检查从内网是否可以登录设备，部署完毕。

1. 443 为 VDC 设备出厂默认的 VPN 监听端口，可以做修改，如做了修改，则端口映射需要映射实际的监听端口。

2.单臂模式必须将设备 LAN 口接到内网交换机。

8.1.4. 单臂多线路模式部署

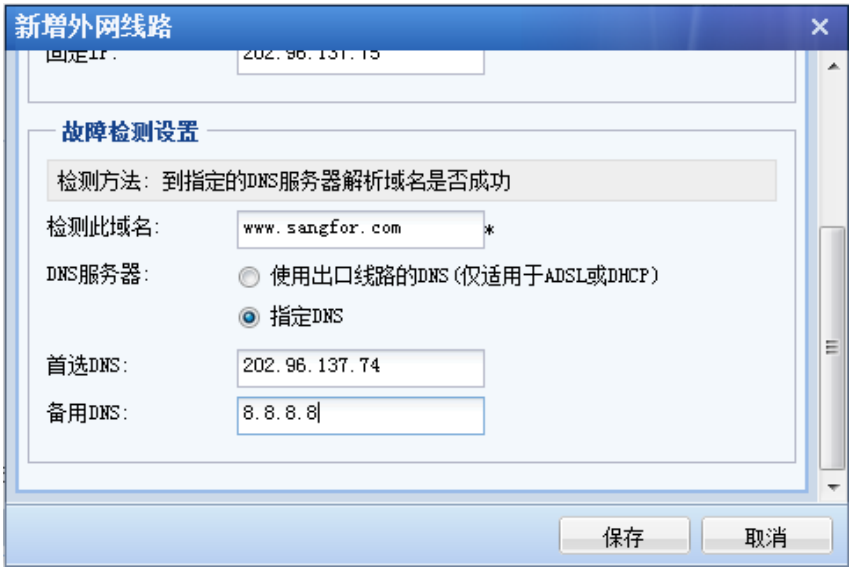
某客户拓扑如图所示，出口有电信与网通两条链路。客户单臂模式部署 VDC 设备，希望实现外网用户输入 202.96.137.75 或者 58.120.10.64 任意一个 IP 地址均能自动选择最快链路接入。



配置步骤如下：

第一步：进入『系统设置』→『网络配置』→『部署模式』，部署模式选择单臂模式，设置好 LAN 口 IP 地址，掩码和网关。界面如下：

第二步：进入『系统设置』→『网络配置』→『多线路』，勾选[启用外网多线路]，并且新增两条外网线路真实的公网 IP 地址。



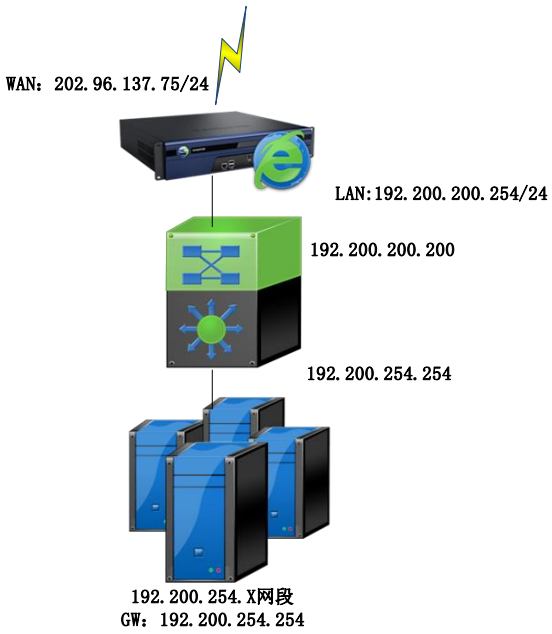
第三步：由于 VDC 设备部署在内网，需要将 VDI 服务对外发布供用户访问，故还需要前置防火墙上做两条线路的 80 端口和 443 端口的端口映射到 VDC 设备。各个厂家设置方法有所不同，此处不截图说明。

以上步骤设置完毕，则可以将设备 LAN 口接到交换机，部署完毕。

VDC 单臂模式部署下必须在前置设备上同时做 HTTPS 端口和 HTTP 端口的映射，默认是 TCP 443 和 80 端口，80 端口的映射也是必须的，否则无法实现多线路智能选路功能。

8.2. 系统路由案例

案例描述：公司内网有两个网段 192.200.200.X 和 192.200.254.X，两个网段通过三层交换机互连互通，VDC 设备网关模式部署，LAN 口 IP 为 192.200.200.254，放在 192.200.200.X 网段，并配置 WAN 口连接 Internet。现 192.200.254.X 和 192.200.200.X 网段都想通过 VDC 设备作为公网出口，共享上网。



由于 192.200.254.X 网段和 VPN 设备的 LAN 口(192.200.200.254)不在同一网段，则 VDC 设备上需要添加系统路由。配置如下：

第一步：进入『防火墙设置』→『NAT 设置』→『代理上网设置』，选择新增，配置需要代理上网的内网网段，界面如下：

第二步：进入『系统设置』→『网络配置』→『路由设置』，添加到 192.200.254.X 网段的路由，界面如下：

8.3. 虚拟门户配置案例

背景需求：同一个客户的不同属性或者不同部门的用户（组）要有自己的个性化登录页面。

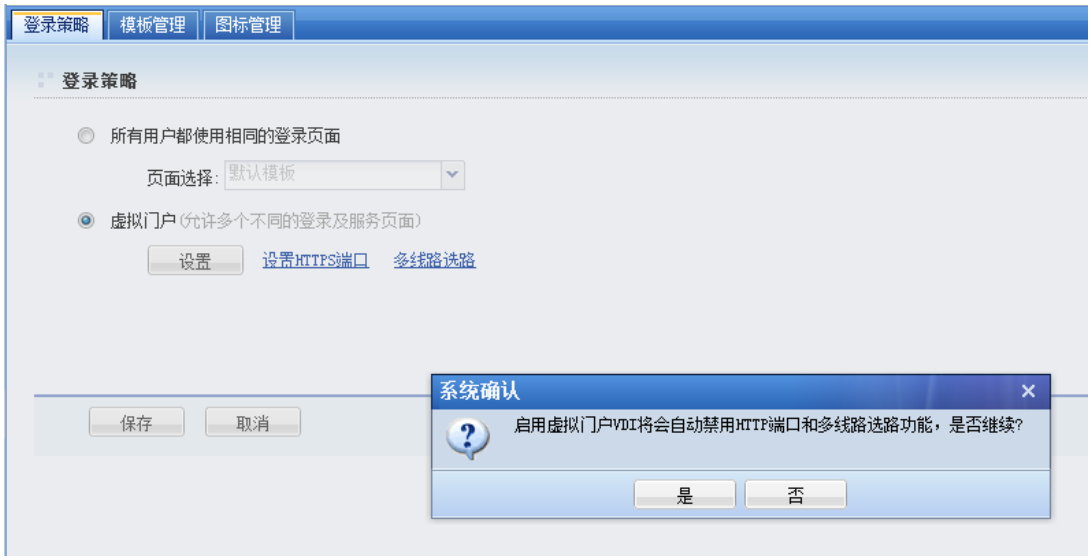
案例：公司的两个部门，市场部和财务部，需要通过 VDC 访问公司内网。但是希望登录时候页面是符合自己部门风格的页面。

实现方法：

第一步：建立两个组，市场部和财务部，分别关联各自需要使用的资源。

第二步：进入『系统设置』→『接入选项』→『EasyConnect』，为两个部门设置登录 VDI 服务的端口，分别为 https 的 445 和 446，界面如下：

第三步：进入『系统设置』→『登录策略』→『登录策略』，开启虚拟门户，弹出如下页面：



点击是之后，点击设置按钮。

此时，点击新建按钮，新建两条登录策略，分别为市场部和财务部选择与其风格对应的页面模板（可以使用系统自带的模板，也可以自定义页面模板），界面如下：

市场部登录策略：

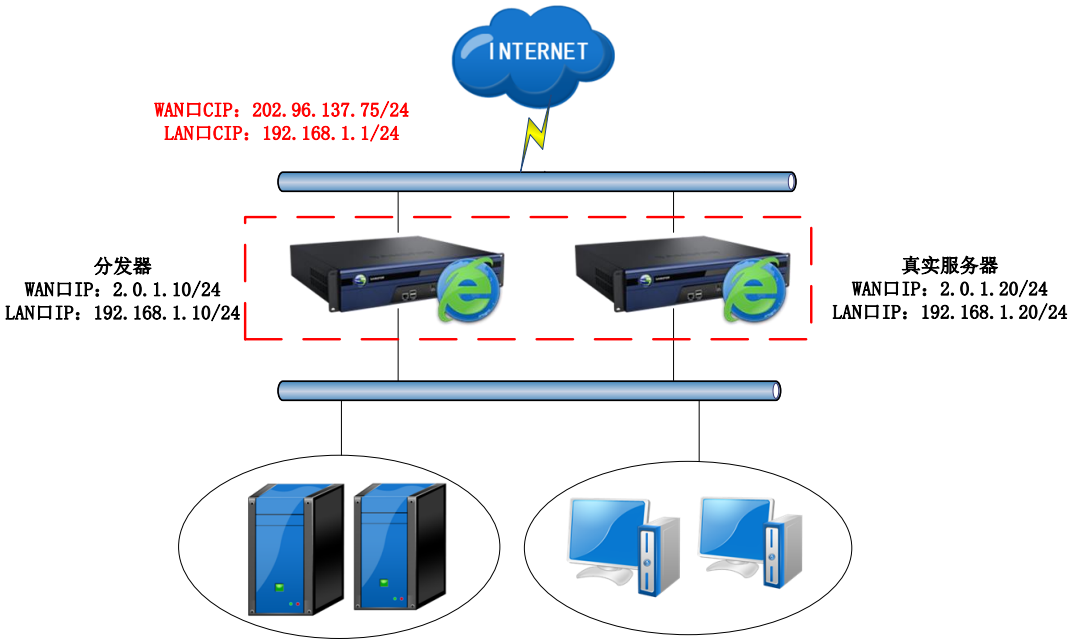
财务部登录策略：

第四步：分别用 HTTPS 的 445 和 446 登录，可以体验到不同的风格。

8.4. 负载均衡集群部署案例

8.4.1. 网关模式部署集群

某客户为了提高内部系统访问的稳定性，采用集群部署 VDC 设备。客户网络拓扑如下，VDC 设备以网关模式部署在客户网络出口处，外网单线路，外网线路地址为 202.96.137.75，子网掩码 255.255.255.0。



网关模式负载均衡集群配置步骤：

第一步：按照网络拓扑将设备部署正确，并且保证分发器和真实服务器的 WAN 口之间可以互相连通，LAN 口之间可以互相连通。

第二步：配置分发器和真实服务器的工作模式、外网接口、内网接口。

分发器：在『系统设置』→『网络配置』→『部署模式』中配置网口，选择『网关模式』。LAN 口设置 IP 地址为 192.168.1.10，子网掩码 255.255.255.0；WAN 口设置 IP 为 2.0.1.10，子网掩码 255.255.255.0，默认网关 2.0.1.254，主备 DNS 必须填写正确的 DNS。

真实服务器：在『系统设置』→『网络配置』→『部署模式』中配置网口，选择『网关模式』。LAN 口设置 IP 地址为 192.168.1.20，子网掩码 255.255.255.0；WAN 口设置 IP 为 2.0.1.20，子网掩码 255.255.255.0，默认网关 2.0.1.254，主备 DNS 必须填写正确的 DNS。

第三步：在『系统设置』→『集群部署』→『集群部署设置』中勾选『启用集群部署功能』，并且设置『集群部署密钥』。

分发器和真实服务器必须都勾选『启用集群部署功能』，并且设置相同的『集群部署密钥』。

第四步：设置分发器选举规则。

如果已经指定了分发器，那么直接在这台设备上选择『优先作为分发器』，其他的设备只能成为真实服务器，必须选择『通过优先级选举分发器』。

如果没有指定分发器，每一台设备都选择『通过优先级选举分发器』，并设置优先级数值，那么该数值越小，优先级越高，优先级最高的设备成为分发器。

第五步：设置 LAN 口集群 IP 和 WAN 口集群 IP。

分发器：LAN 口集群 192.168.1.1，LAN 口集群掩码 255.255.255.0；WAN1 口集群 IP 填写真实的外网 IP 地址 202.96.137.75，WAN1 口集群掩码 255.255.255.0，WAN1 口网关 202.96.137.254。

真实服务器：LAN 口集群 192.168.1.1，LAN 口集群掩码 255.255.255.0；WAN1 口集群 IP 填写真实的外网 IP 地址 202.96.137.75，WAN1 口集群掩码 255.255.255.0，WAN1 口网关 202.96.137.254。

 **注意：LAN 口集群 IP 和每台设备内网接口设置的 IP 必须在同一个网段。每台设备的外网接口可以设置任意网段的 IP，但两台设备的外网接口 IP 必须在同一网段，外网接口的网关可以任意填写（不能全填 0）。WAN 口集群 IP 必须和每台设备在外网接口设置的 IP 不在同一个网段。**

注意：若 VDC 设备做网关，则 VDC 设备不能用拨号上网。

第六步：在『系统设置』→『集群部署』→『集群部署状态』中查看集群运行状态。

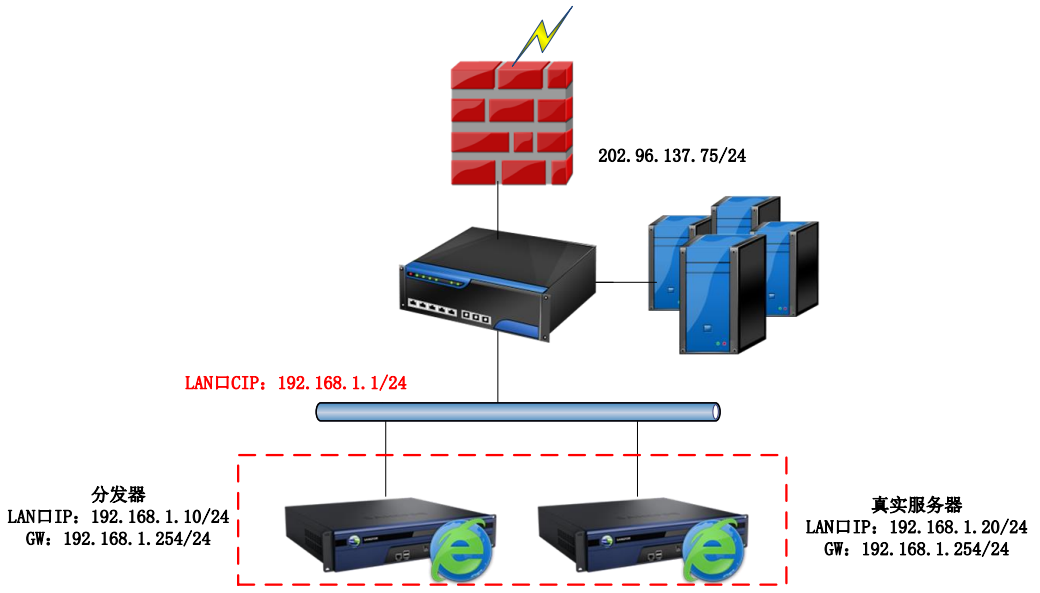
这里可以显示集群中分发器和真实服务器的各种实时状态信息，包括节点 IP，节点类型，VDI 服务运行状态，各个节点的 CPU 使用率，各个节点的在线人数，各个节点的授权数，总在线人数，总授权数等。

第七步：在『系统设置』→『集群部署』→『集群在线用户』中查看当前接入 VDC 设备的用户名称、接入 IP、接入时间等，并可以对接入的用户进行断开连接操作。

第八步：配置完成。

8.4.2. 单臂模式部署集群

某客户为了提高内部系统访问的稳定性，采用集群部署 VDC 设备。客户网络拓扑如下，VDC 设备以单臂模式部署在客户网络出口处，外网单线路，外网线路地址为 202.96.137.75，子网掩码 255.255.255.0。



单臂模式负载均衡集群配置步骤：

第一步：按照网络拓扑将设备部署正确，WAN 口不用接线，并且保证分发器和真实服务器的 LAN 口之间可以互相连通。

第二步：配置分发器和真实服务器的工作模式、内网接口。

分发器：在『系统设置』→『网络配置』→『部署模式』中配置网口，选择『单臂模式』。LAN 口设置 IP 地址为 192.168.1.10，子网掩码 255.255.255.0；默认网关填写 192.168.1.254；主备 DNS 必须填写正确的 DNS。

真实服务器：在『系统设置』→『网络配置』→『部署模式』中配置网口，选择『单臂模式』。LAN 口设置 IP 地址为 192.168.1.20，子网掩码 255.255.255.0；默认网关填写 192.168.1.254；主备 DNS 必须填写正确的 DNS。

第三步：在『系统设置』→『集群部署』→『集群部署设置』中勾选『启用集群部署功能』，并且设置『集群部署密钥』。

分发器和真实服务器必须都勾选『启用集群部署功能』，并且设置相同的『集群部署密钥』。

第四步：设置分发器选举规则。

如果已经指定了分发器，那么直接在这台设备上选择『优先作为分发器』，其他的设备只能成为真实服务器，必须选择『通过优先级选举分发器』。

如果没有指定分发器，每一台设备都选择『通过优先级选举分发器』，并设置优先级数值，那么该数值越小，优先级越高，优先级最高的设备成为分发器。

第五步：设置 LAN 口集群 IP。

分发器：LAN 口集群 192.168.1.1，LAN 口集群掩码 255.255.255.0。

真实服务器：LAN 口集群 192.168.1.1，LAN 口集群掩码 255.255.255.0。

注意：LAN 口集群 IP 和每台设备内网接口设置的 IP 必须在同一个网段。

 **注意：VDC 设备集群不支持动态 IP，前置网关设备不能用拨号上网。**

第六步：前置网关设备做端口映射，将 202.96.137.75 的 TCP443、80 端口映射给内网的 LAN 口集群 IP192.168.1.1。

第七步：在『系统设置』→『集群部署』→『集群部署状态』中查看集群运行状态。

这里可以显示集群中分发器和真实服务器的各种实时状态信息，包括节点 IP，节点类型，VDI 服务运行状态，各个节点的 CPU 使用率，各个节点的在线人数，各个节点的授权数，总在线人数，总授权数等。

第八步：在『系统设置』→『集群部署』→『集群在线用户』中查看当前接入 VDC 设备的用户名称、接入 IP、接入时间等，并可以对接入的用户进行断开连接操作。

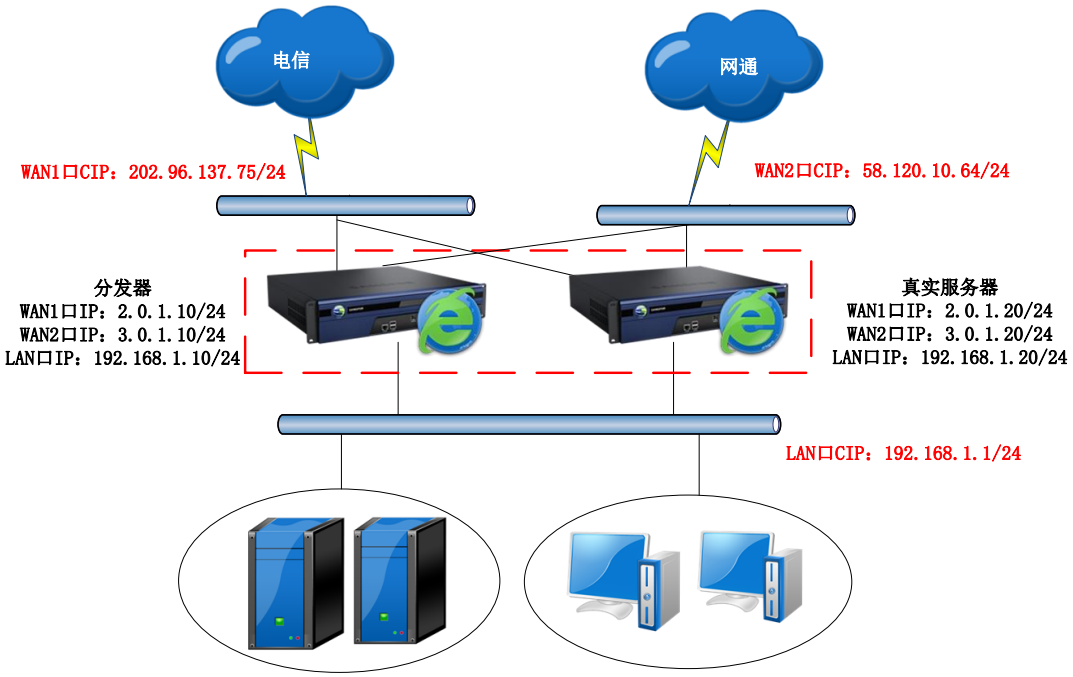
第九步：配置完成。

8.4.3. 网关模式多线路集群部署

某客户为了提高内部系统访问的稳定性，采用集群部署 VDC 设备。客户网络拓扑如下，VDC 设备以网关模式部署在客户网络出口处，外网双线路。

外网电信线路地址为 202.96.137.75，子网掩码 255.255.255.0。

外网网通线路地址为 58.120.10.64，子网掩码 255.255.255.0。



网关模式多线路负载均衡集群配置步骤：

第一步：按照网络拓扑将设备部署正确，每个设备的 WAN1 口和 WAN2 口分别接两条外网线路，并且保证分发器和真实服务器的 WAN1 口之间可以互相连通，WAN2 口之间可以互相连通，LAN 口之间可以互相连通。

第二步：配置分发器和真实服务器的工作模式、外网接口、内网接口。

分发器：在『系统设置』→『网络配置』→『部署模式』中配置网口，选择『网关模式』。LAN 口设置 IP 地址为 192.168.1.10，子网掩码 255.255.255.0；外网线路 1，WAN1 口设置 IP 为 2.0.1.10，子网掩码 255.255.255.0，默认网关 2.0.1.254，主备 DNS 必须填写正确的 DNS；外网线路 2，WAN2 口设置 IP 为 3.0.1.10，子网掩码 255.255.255.0，默认网关 3.0.1.254，主备 DNS 必须填写正确的 DNS；

真实服务器：在『系统设置』→『网络配置』→『部署模式』中配置网口，选择『网关模式』。LAN 口设置 IP 地址为 192.168.1.20，子网掩码 255.255.255.0；外网线路 1，WAN1 口设置 IP 为 2.0.1.20，子网掩码 255.255.255.0，默认网关 2.0.1.254，主备 DNS 必须填写正确的 DNS；外网线路 2，WAN2 口设置 IP 为 3.0.1.20，子网掩码 255.255.255.0，

默认网关 3.0.1.254，主备 DNS 必须填写正确的 DNS；

第三步：在『系统设置』→『网络配置』→『多线路』中，勾选[启用外网多线路传输]，并且设置好两条线路；然后勾选[启用多线路]，建议分发器和真实服务器都启用多线路自动选路。

第四步：在『系统设置』→『集群部署』→『集群部署设置』中勾选『启用集群部署功能』，并且设置『集群部署密钥』。

分发器和真实服务器必须都勾选『启用集群部署功能』，并且设置相同的『集群部署密钥』。

第五步：设置分发器选举规则。

如果已经指定了分发器，那么直接在这台设备上选择『优先作为分发器』，其他的设备只能成为真实服务器，必须选择『通过优先级选举分发器』。

如果没有指定分发器，每一台设备都选择『通过优先级选举分发器』，并设置优先级数值，那么该数值越小，优先级越高，优先级最高的设备成为分发器。

第六步：设置 LAN 口集群 IP 和 WAN 口集群 IP。

分发器：LAN 口集群 192.168.1.1，LAN 口集群掩码 255.255.255.0；WAN1 口集群 IP 填写真实的外网 IP 地址 202.96.137.75，WAN1 口集群掩码 255.255.255.0，WAN1 口网关 202.96.137.254；WAN2 口集群 IP 填写真实的外网 IP 地址 58.120.10.64，WAN1 口集群掩码 255.255.255.0，WAN1 口网关 58.120.10.254；

真实服务器：LAN 口集群 192.168.1.1，LAN 口集群掩码 255.255.255.0；WAN1 口集群 IP 填写真实的外网 IP 地址 202.96.137.75，WAN1 口集群掩码 255.255.255.0，WAN1 口网关 202.96.137.254；WAN2 口集群 IP 填写真实的外网 IP 地址 58.120.10.64，WAN1 口集群掩码 255.255.255.0，WAN1 口网关 58.120.10.254；

 **注意：LAN 口集群 IP 和每台设备内网接口设置的 IP 必须在同一个网段。每台设备**

的外网接口可以设置任意网段的 IP，但两台设备的外网接口 IP 必须在同一网段，外网接口的网关可以任意填写（不能全填 0）。WAN 口集群 IP 必须和每台设备在外网接口设置的 IP 不在同一个网段。

 **注意：若 VDC 设备做网关，则 VDC 设备不能用拨号上网。**

第七步：在『系统设置』→『集群部署』→『集群部署状态』中查看集群运行状态。

这里可以显示集群中分发器和真实服务器的各种实时状态信息，包括节点 IP，节点类型，VDI 服务运行状态，各个节点的 CPU 使用率，各个节点的在线人数，各个节点的授权数，总在线人数，总授权数等。

第八步：在『系统设置』→『集群部署』→『集群在线用户』中查看当前接入 VDC 设备的用户名称、接入 IP、接入时间等，并可以对接入的用户进行断开连接操作。

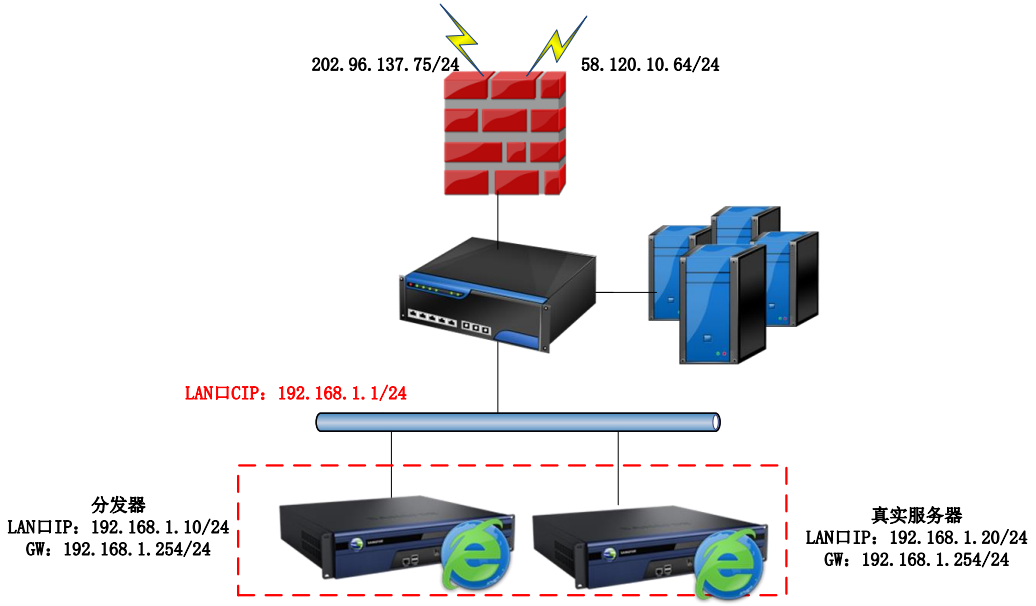
第九步：配置完成。

8.4.4. 单臂模式多线路集群部署

某客户为了提高内部系统访问的稳定性，采用集群部署 VDC 设备。客户网络拓扑如下，VDC 设备以单臂模式部署在客户网络出口处，外网双线路。

外网电信线路地址为 202.96.137.75，子网掩码 255.255.255.0。

外网网通线路地址为 58.120.10.64，子网掩码 255.255.255.0。



单臂模式多线路负载均衡集群配置步骤：

第一步：按照网络拓扑将设备部署正确，WAN 口不用接线，并且保证分发器和真实服务器的 LAN 口之间可以互相连通。

第二步：配置分发器和真实服务器的工作模式、内网接口。

分发器：在『系统设置』→『网络配置』→『部署模式』中配置网口，选择『单臂模式』。LAN 口设置 IP 地址为 192.168.1.10，子网掩码 255.255.255.0；默认网关填写 192.168.1.254；主备 DNS 必须填写正确的 DNS。

真实服务器：在『系统设置』→『网络配置』→『部署模式』中配置网口，选择『单臂模式』。LAN 口设置 IP 地址为 192.168.1.20，子网掩码 255.255.255.0；默认网关填写 192.168.1.254；主备 DNS 必须填写正确的 DNS。

第三步：在『系统设置』→『网络配置』→『多线路』中，勾选[启用外网多线路]，并且新增两条线路，填写外网线路真实的公网 IP 地址；建议分发器和真实服务器都启用多线路自动选路。

分发器：新增外网线路。填写外网线路 1 的 IP 地址 202.96.137.75、HTTP 端口 80、

HTTPS 端口 443；填写外网线路 2 的 IP 地址 58.120.10.64、HTTP 端口 80、HTTPS 端口 443。

真实服务器：新增外网线路。填写外网线路 1 的 IP 地址 202.96.137.75、HTTP 端口 80、HTTPS 端口 443；填写外网线路 2 的 IP 地址 58.120.10.64、HTTP 端口 80、HTTPS 端口 443。

 **注意：若使用单臂多线路部署必须启用该选项，并且正确配置前端多线路的信息。**

第四步：在『系统设置』→『集群部署』→『集群部署设置』中勾选『启用集群部署功能』，并且设置『集群部署密钥』。

分发器和真实服务器必须都勾选『启用集群部署功能』，并且设置相同的『集群部署密钥』。

第五步：设置分发器选举规则。

如果已经指定了分发器，那么直接在这台设备上选择『优先作为分发器』，其他的设备只能成为真实服务器，必须选择『通过优先级选举分发器』。

如果没有指定分发器，每一台设备都选择『通过优先级选举分发器』，并设置优先级数值，那么该数值越小，优先级越高，优先级最高的设备成为分发器。

第六步：设置 LAN 口集群 IP。

分发器：LAN 口集群 192.168.1.1，LAN 口集群掩码 255.255.255.0。

真实服务器：LAN 口集群 192.168.1.1，LAN 口集群掩码 255.255.255.0。

 **注意：LAN 口集群 IP 和每台设备内网接口设置的 IP 必须在同一个网段。**

 **注意：VDC 设备集群不支持动态 IP，前置网关设备不能用拨号上网。**

第七步：前置网关设备做端口映射，将 202.96.137.75 的 TCP443、80 端口映射给内

网的 LAN 口集群 IP192.168.1.1；将 58.120.10.64 的 TCP443、80 端口映射给内网的 LAN 口集群 IP192.168.1.1。

第八步：在『系统设置』→『集群部署』→『集群部署状态』中查看集群运行状态。

这里可以显示集群中分发器和真实服务器的各种实时状态信息，包括节点 IP，节点类型，VDI 服务运行状态，各个节点的 CPU 使用率，各个节点的在线人数，各个节点的授权数，总在线人数，总授权数等。

第九步：在『系统设置』→『集群部署』→『集群在线用户』中查看当前接入 VDC 设备的用户名称、接入 IP、接入时间等，并可以对接入的用户进行断开连接操作。

第十步：配置完成。

8.5. 新建用户配置案例

案例目标 1：建立一个采用用户名密码认证的用户，用户名为 ww，密码为 123。

配置步骤如下：

第一步：进入『VDI 设置』→『用户管理』页面，点击新建按钮，新增用户，界面如下图所示：

第二步：在用户信息编辑页面，设置用户的账号和密码。本例中用户名为 ww，密码为 123，『主要认证』选择[用户名/密码]，如下图所示：

设置好之后，点击保存按钮，再点击立即生效按钮，就可以用这个账号登录 VDI 了。

案例目标 2：建立一个采用数字证书认证的用户。

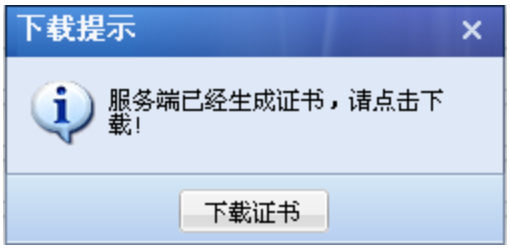
配置步骤如下：

第一步：进入『VDI 设置』→『用户管理』页面，点击新建按钮，新增用户，界面如下图所示：

第二步：在用户信息编辑页面，建立一个数字证书用户。名称为“support”，用户类型为[私有用户]，主要认证方式勾选[数字证书/Dkey 认证]，界面如下图所示：

点击生成证书，界面如下图所示：

点击开始生成，界面如下图所示：



点击下载证书，并把证书保存在本地。

第三步：安装证书，登录 VDI。双击保存的 support.p12 证书，安装之后，打开登录界面，点击证书登录即可。

8.6. 资源配置案例

8.6.1. 远程应用配置案例

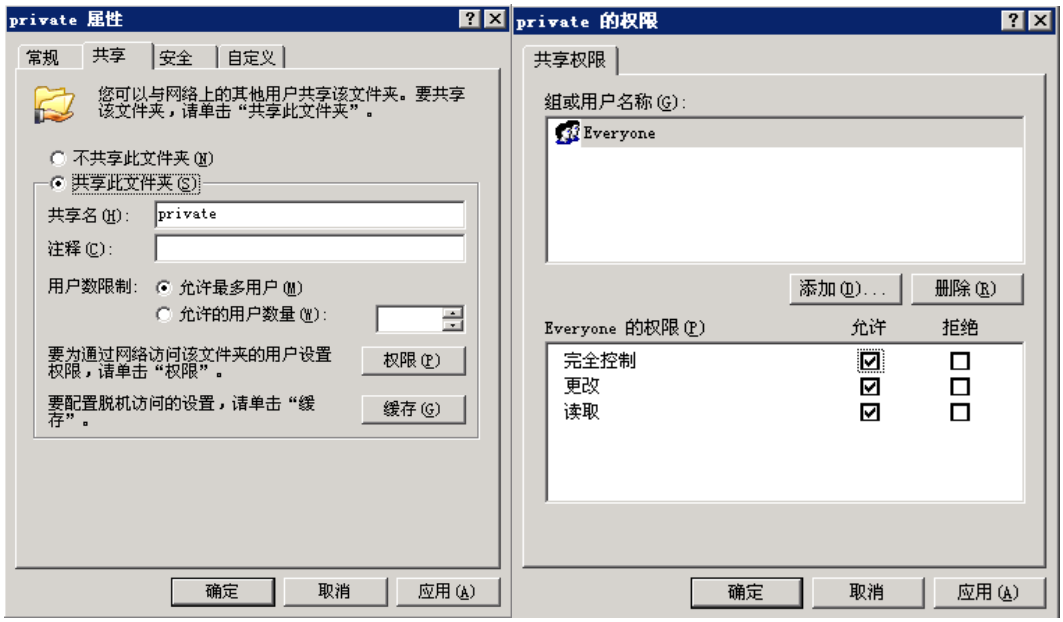
案例背景：某公司通过 VDC 设备远程发布了一个写字板程序，并要求用户能将修改后的文档存储在服务器上的私有文件夹里，也能够将修改后的文档存储在服务器上的公有文件夹里。

配置步骤如下：

第一步：在终端服务器和存储服务器上安装终端服务和 RemoteAppAgent 程序。

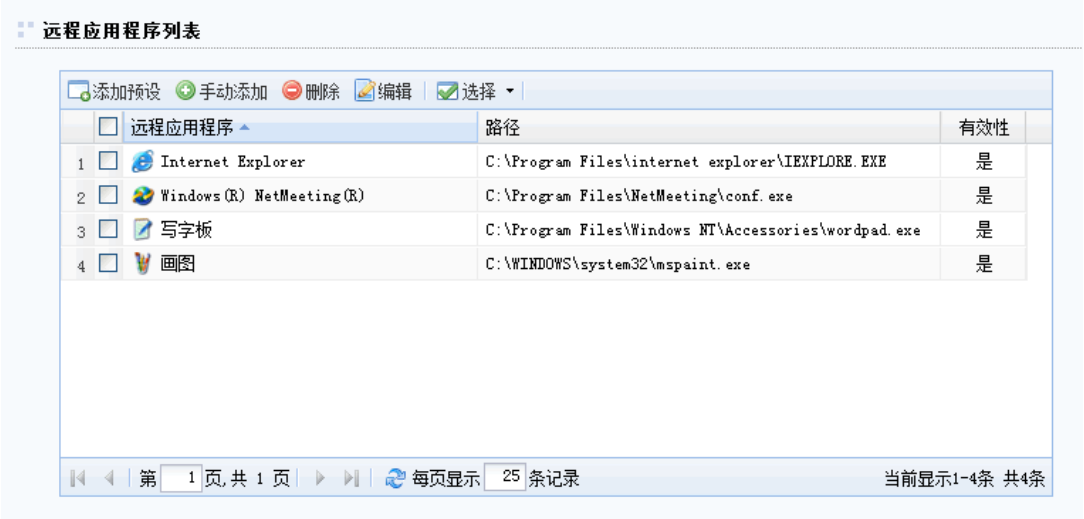
RemoteAppAgent 程序下载位置『VDI 设置』→『服务器管理』-『下载终端服务器程序』：

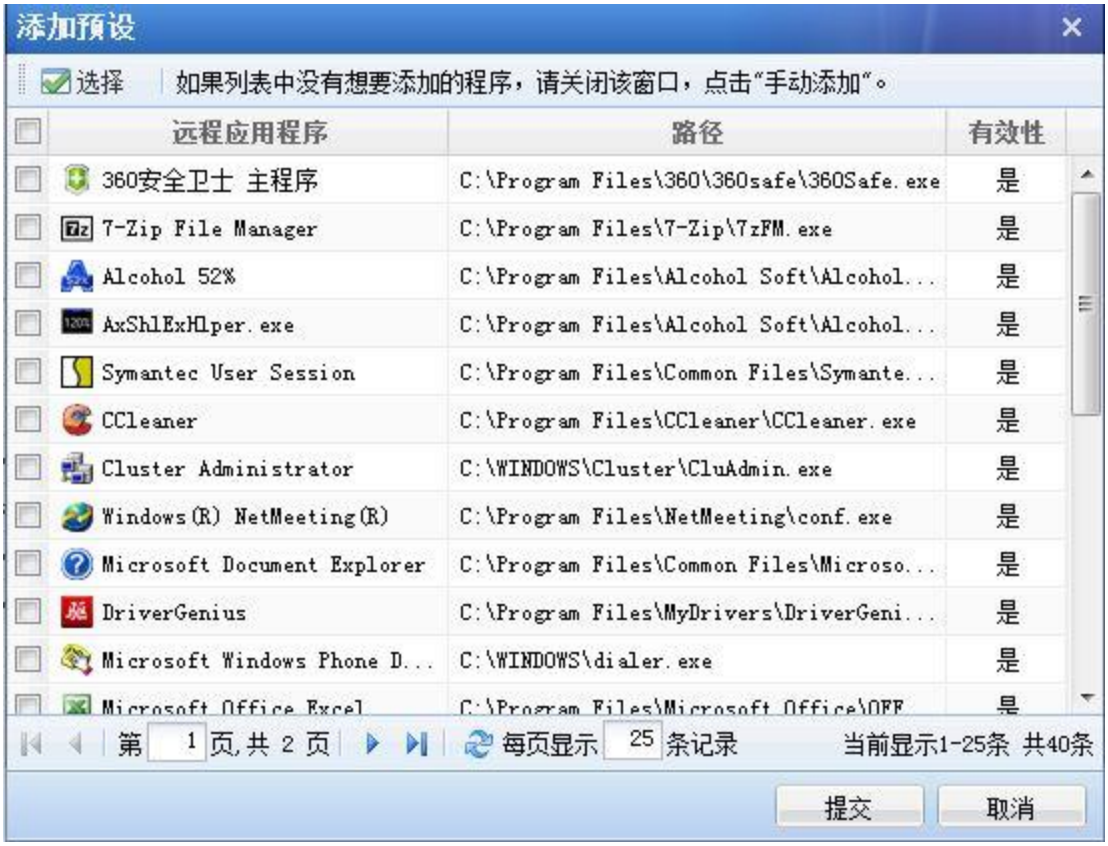
第二步：在存储服务器上创建个人目录和公共目录，要求目录文件夹为 NTFS 格式且设置为共享文件夹，并设置文件夹的访问权限。



第三步：进入『VDI 设置』→『服务器管理』页面，点击新增，新增资源服务器，在资源服务器里添加需要发布的应用程序的预设。

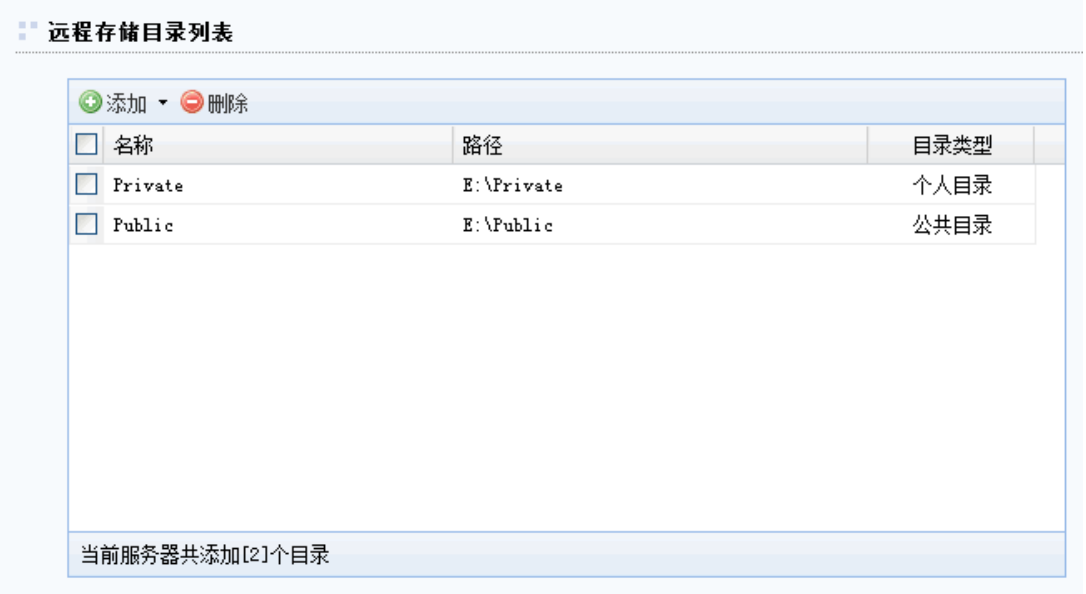
在【远程应用程序列表】中点击添加预设，如下图所示：





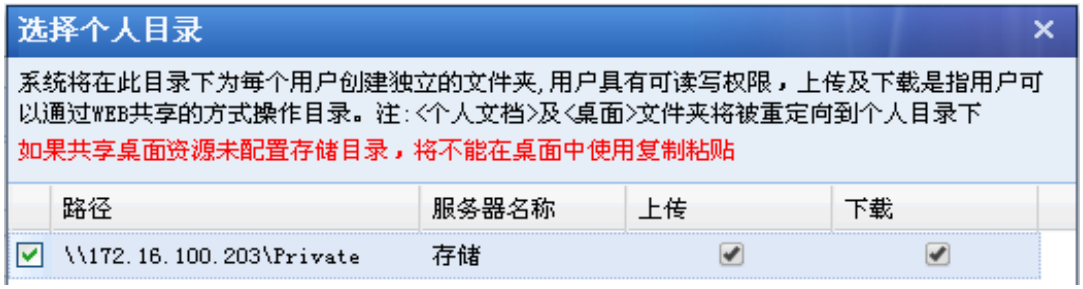
在这里会显示出终端服务器上面的所有进程，勾选需要提供给用户使用的服务，点击提交即可，这里需要发布的是写字板程序。

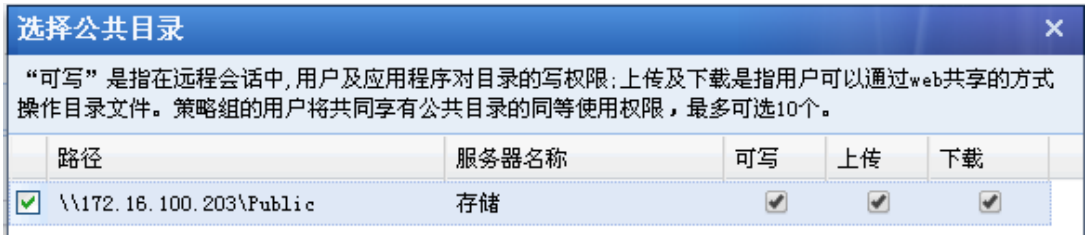
点击新增，新增存储服务器，在存储服务器里添加需要保存文件的共享文件夹。



第四步：进入『VDI 设置』→『策略组管理』页面，新增策略组。选择“远程应用与共享桌面”，设置账号接入属性以及用户的存储目录。

点击个人目录和公共目录的  按钮，选择相应的存储目录，界面如下图所示：





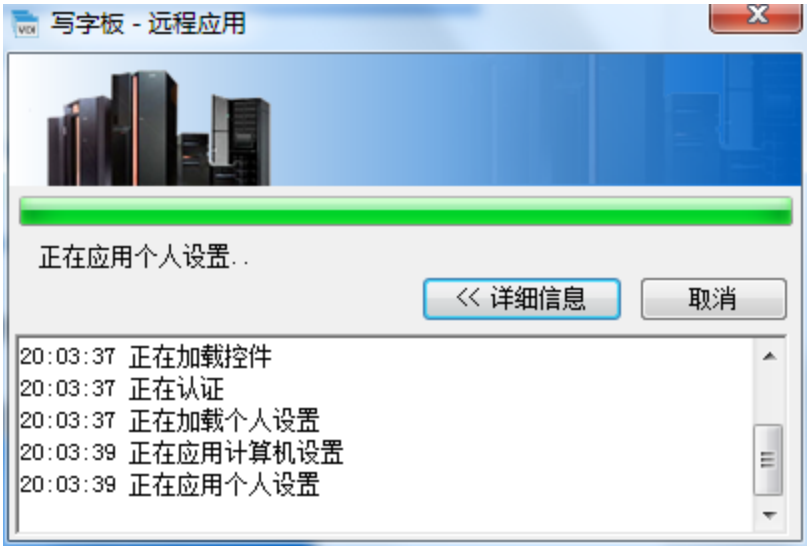
第五步：进入『VDI 设置』→『用户管理』页面，新建接入用户，关联策略组。

第六步：进入『VDI 设置』→『资源管理』页面，新建远程应用，添加需要发布的应用。

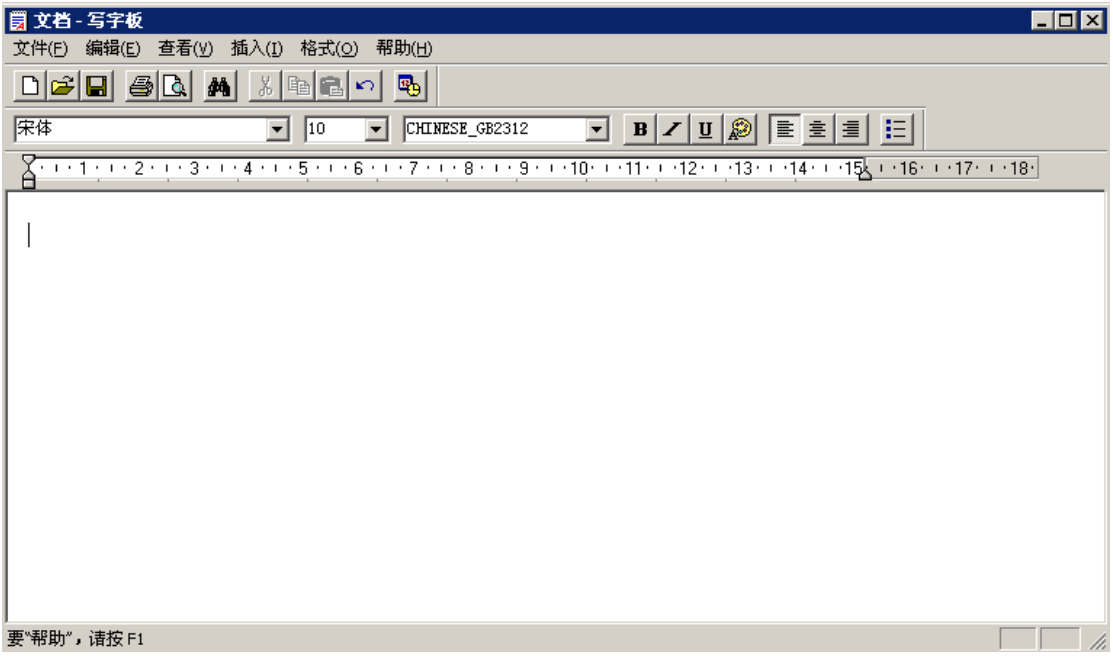
第七步：进入『VDI 设置』→『角色授权』页面，关联用户和资源。

第八步：配置完成。使用 XXL 账号登录 VDI 后的效果展示：

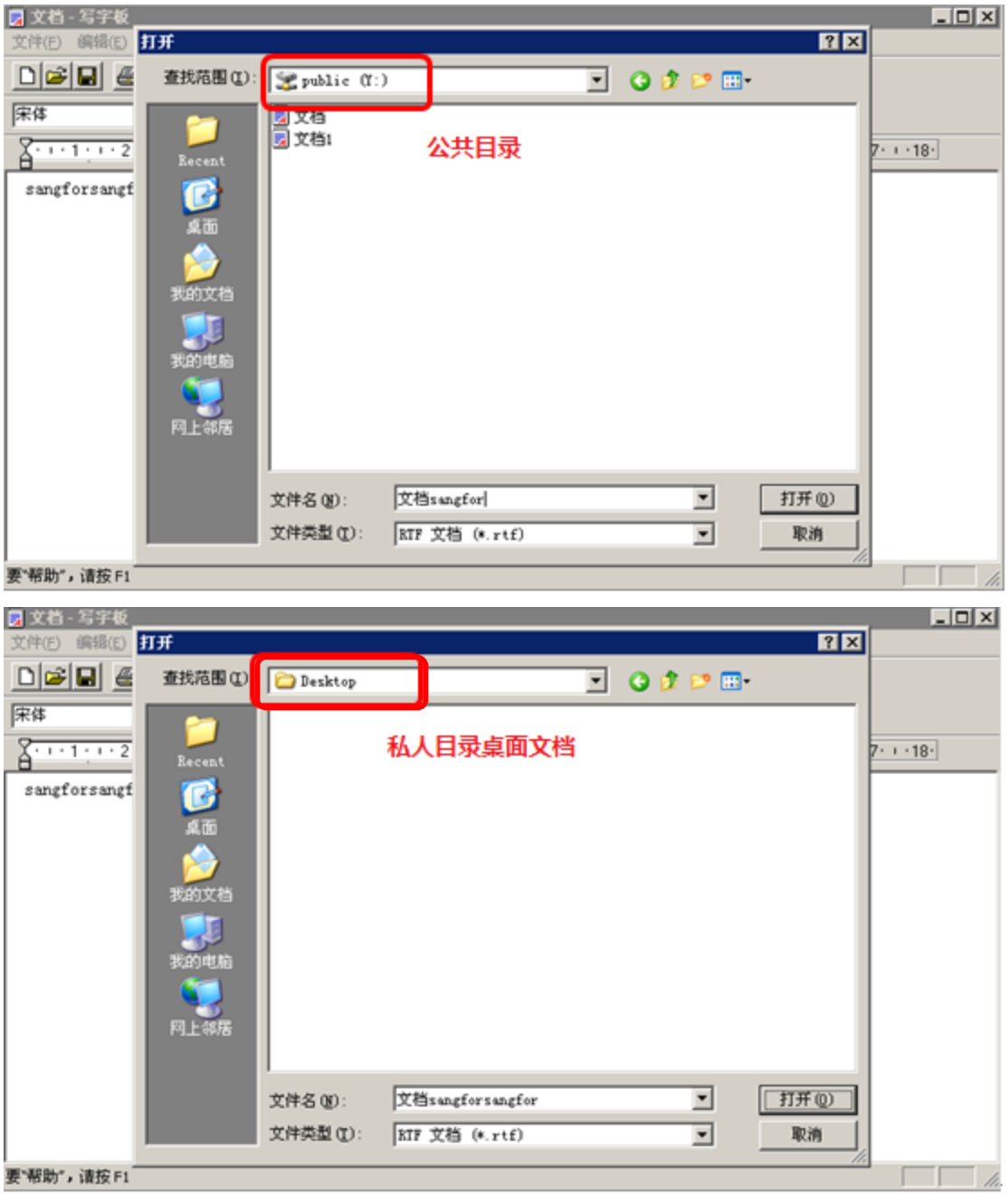
（1）点击资源名称，启用远程应用服务，如下图所示：



启动会话进程完成后，可以正常打开应用程序--写字板



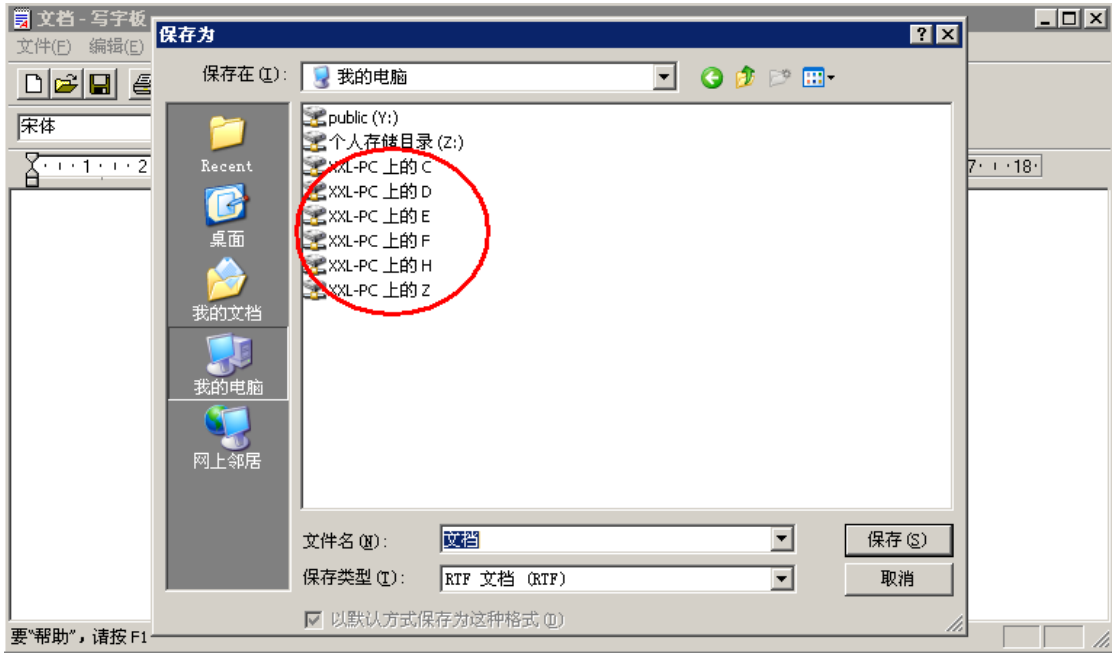
（2）写字板中编辑文字，编辑后能够保存到个人目录和公共目录里。



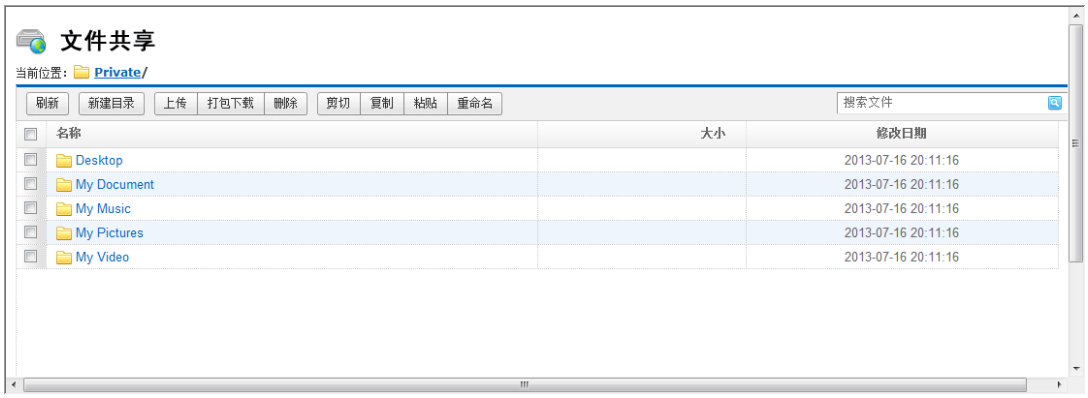
（3）若需要将修改后的文档保存在客户端的电脑上。

方法一：在策略组里勾选“本地磁盘映射”并在客户端远程应用设置里勾选“本地驱动器”，重新登录 VDI 进行测试。

此时，点击保存，就可以看到本地磁盘。



方法二：通过文件共享的方式下载到本地



但是要求在选择个人目录或公共目录时勾选上“下载”，上传也是一样的。

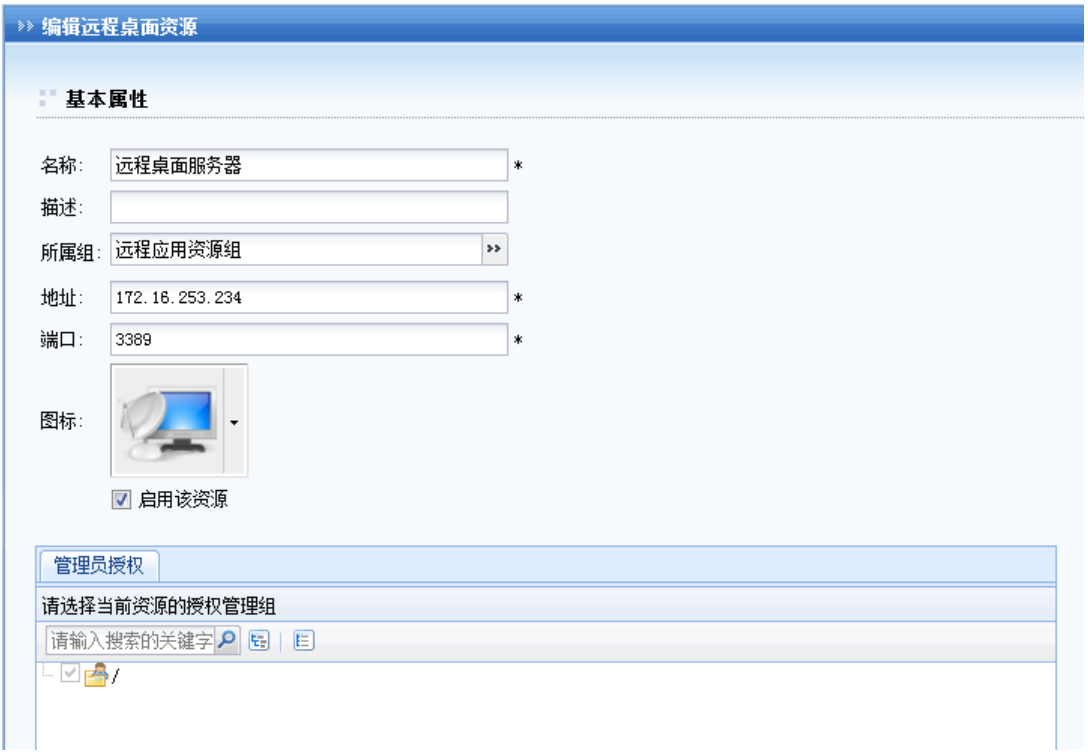
8.6.2. 远程桌面配置案例

案例背景：某公司通过 VDC 设备远程发布了一个远程桌面服务器，用户可以通过 VDI 接入远程桌面进行办公上网，如同在内网进行操作一样。

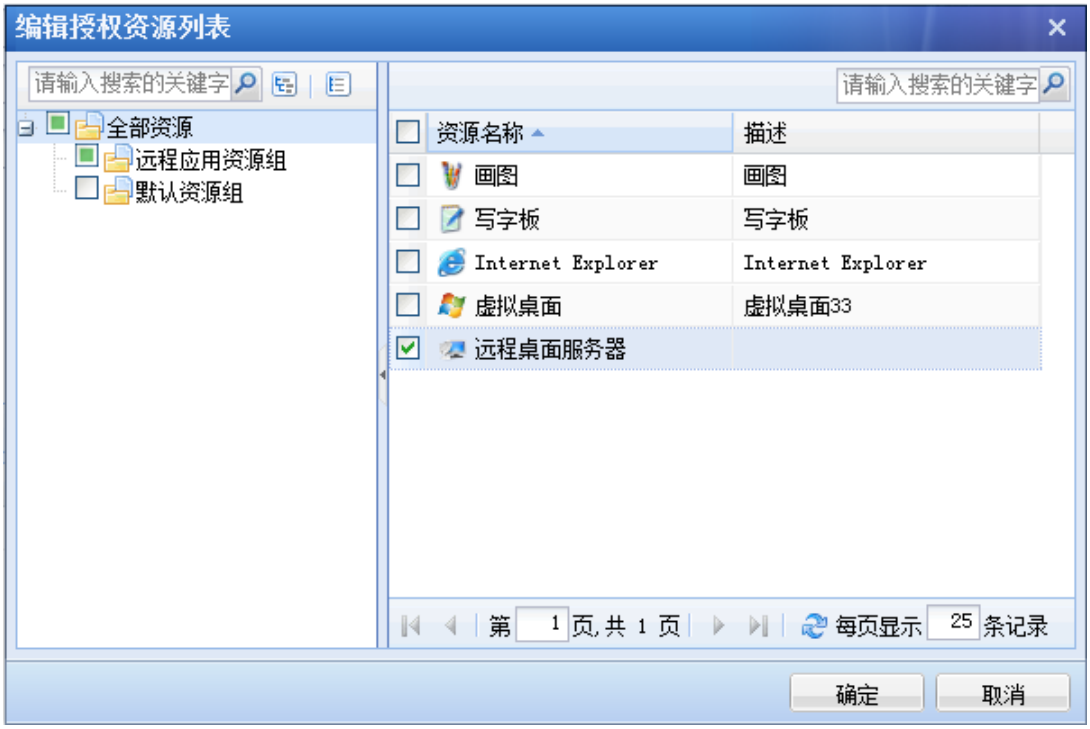
配置步骤如下：

第一步：在服务器上开通远程桌面服务，如有需要，请设置防火墙允许访问其 3389 远程桌面服务端口。

第二步：进入『VDI 设置』→『资源管理』页面，新建远程桌面资源，添加需要发布的远程桌面服务器，填入服务器的 IP 和端口，端口默认为 3389。



第三步：进入『VDI 设置』→『角色授权』页面，关联用户和资源。



第八步：配置完成。使用 XXL 账号登录后的效果展示：

（1）点击资源名称，启用远程桌面，第一次使用，需要关联远程桌面程序。需要选择 mstsc.exe 所在的路径。如下图所示：

（2）设置完成后即可启动远程桌面连接，通过远程桌面连接到指定的服务器进行操作。

8.6.3. 共享桌面配置案例

案例背景：某公司通过 VDC 设备远程发布了一个终端服务器，用户可以通过 VDI 接入服务器进行办公上网。

配置步骤如下：

第一步：在终端服务器上安装终端服务和 RemoteAppAgent 程序。

RemoteAppAgent 程序下载位置『VDI 设置』→『服务器管理』-『下载终端服务器程序』：

第二步：进入『VDI 设置』→『策略组管理』页面，新增策略组。选择“远程应用与共享桌面”，设置远程账号接入属性以及用户的存储目录。

第三步：进入『VDI 设置』→『用户管理』页面，新建远程应用接入用户，关联远程应用策略组。

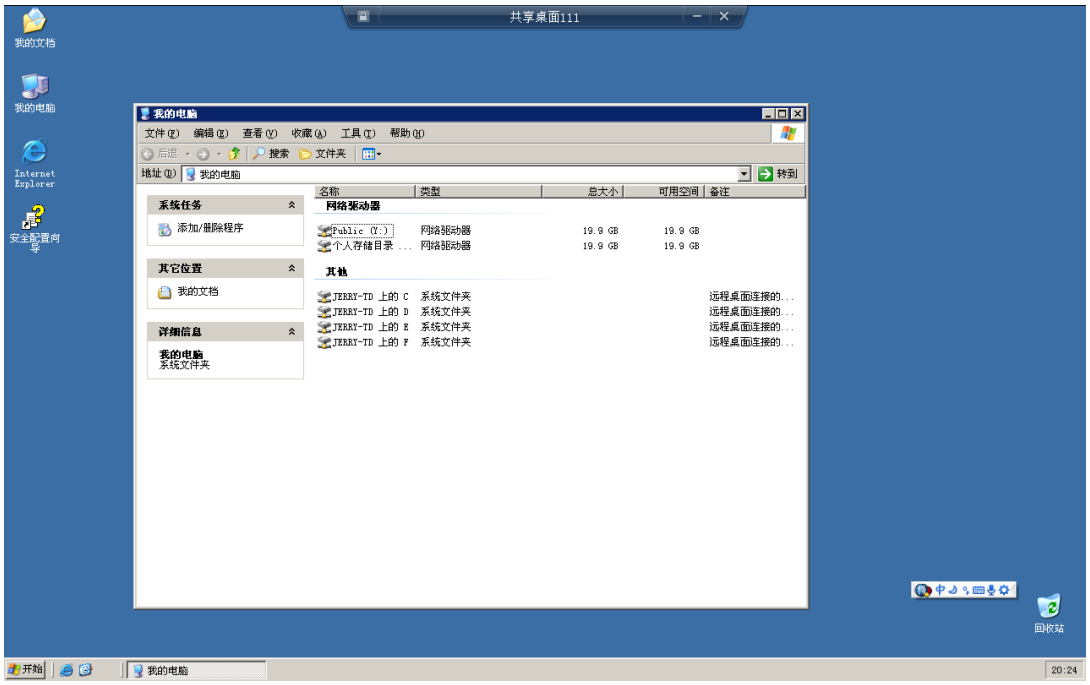
第六步：进入『VDI 设置』→『资源管理』页面，新建共享桌面资源，添加需要发布的终端服务器。

第七步：进入『VDI 设置』→『角色授权』页面，关联用户和资源。

第八步：配置完成。使用 XXL 账号登录后的效果展示：

（1）点击资源名称，启用远程应用服务，如下图所示：

启动会话进程完成后，可以进入共享桌面的视图，打开我的电脑可以看到共享的共用存储目录和个人存储目录。



8.6.4. 独享桌面配置案例

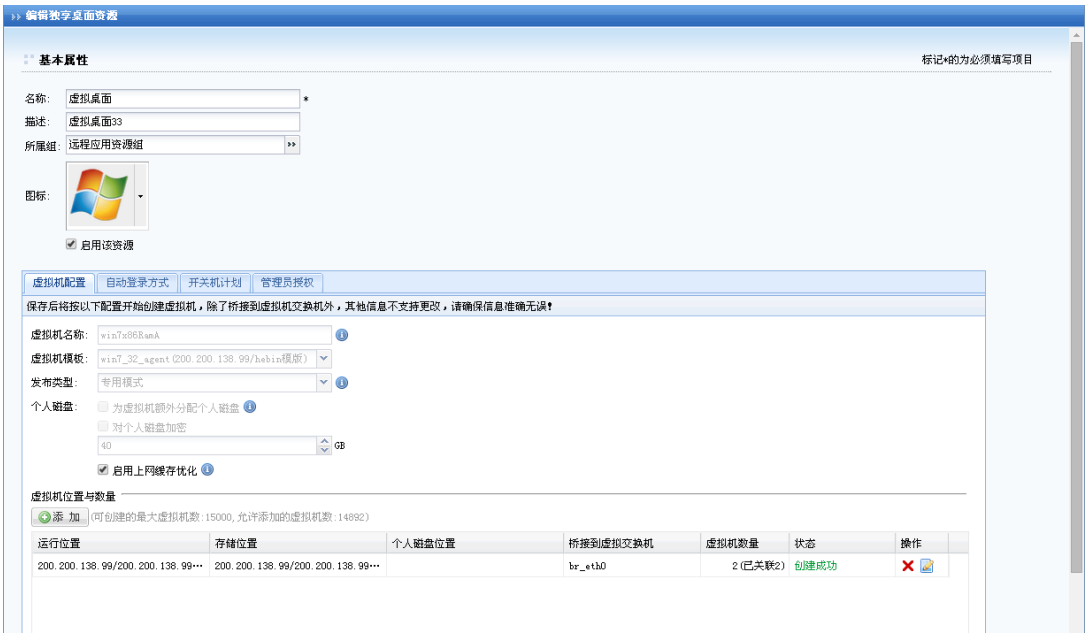
案例背景：某公司安装使用深信服虚拟化平台提供虚拟化服务，通过 VDC 设备远程发布虚拟机，每个用户关联一台虚拟机进行使用。

配置步骤如下：

第一步：添加虚拟化平台控制器。

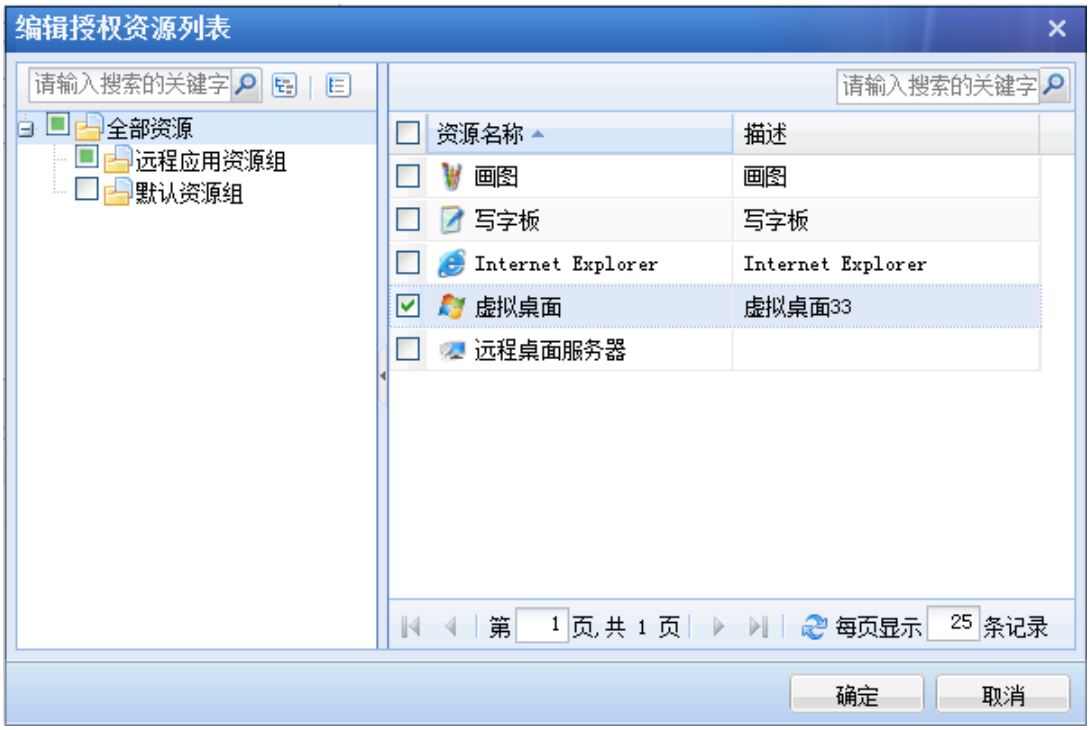
在『VDI 设置』→『虚拟化平台管理』→『虚拟化平台控制器』页面，点击新建以添加虚拟化平台控制器。输入名称、描述和控制器地址、连接账号密码，保存配置。

第二步：添加独享桌面资源。进入『VDI 设置』→『资源管理』页面，新建独享桌面资源，设置虚拟机模版并添加虚拟机。



第三部：添加用户并关联角色。

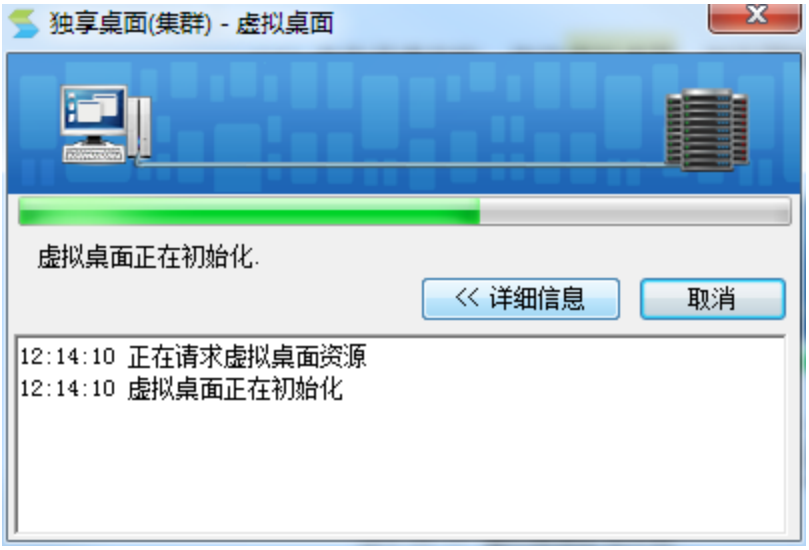
进入『VDI 设置』→『角色授权』页面，关联用户和资源。



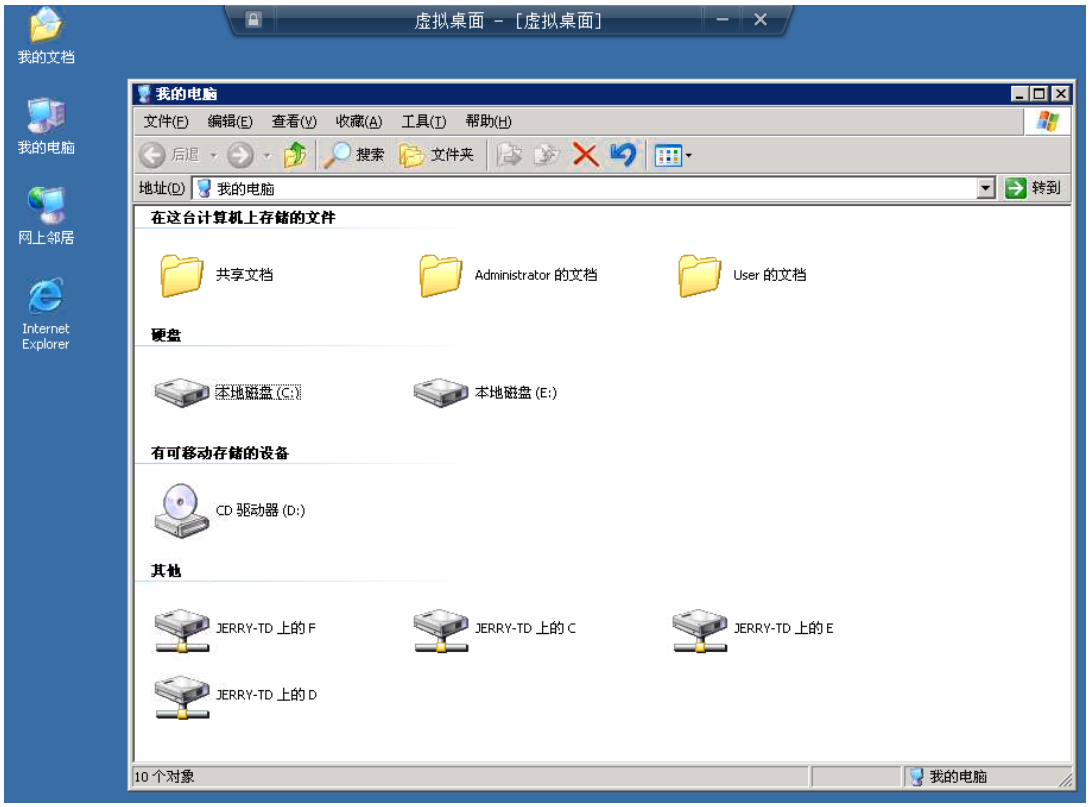
第五步：配置完成。

使用 XXL 账号登录后的效果展示：

（1）点击资源名称，启动独享桌面，如下图所示：



虚拟机开机完成后，自动登录进入独享桌面。



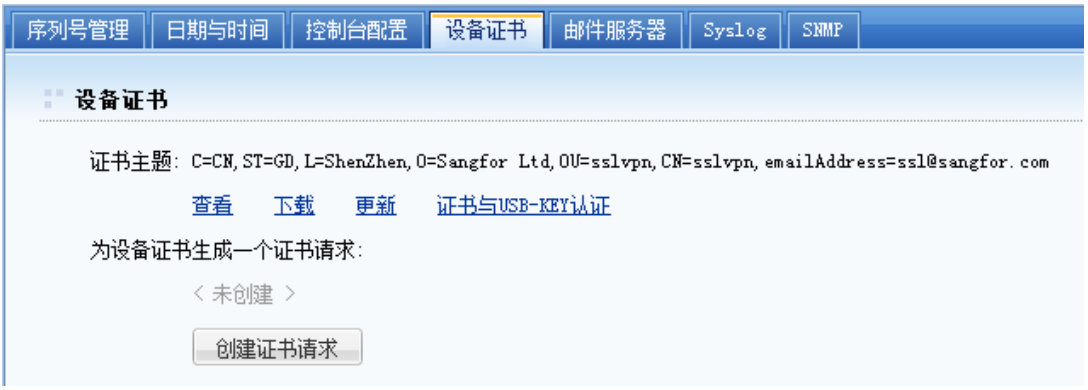
8.7. 外部认证配置案例

8.7.1. 结合第三方 CA 实现数字证书认证

某客户希望 VDC 设备同第三方 CA 结合做数字证书的认证。

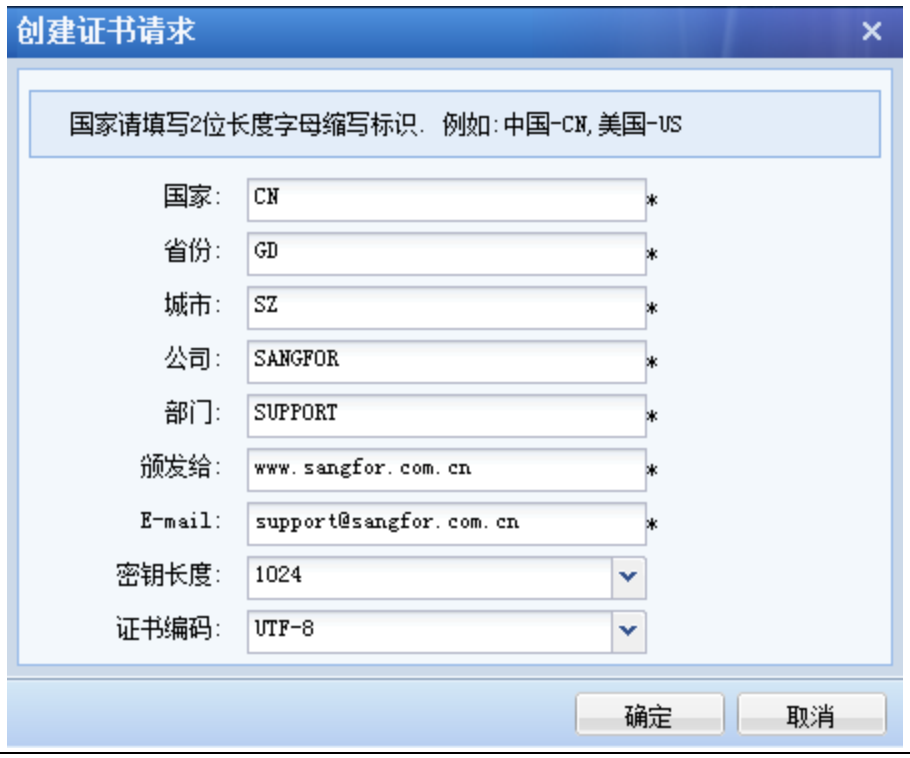
配置步骤如下：

第一步：进入『系统设置』→『系统配置』→『设备证书』页面，生成一个第三方证书请求，页面如下图所示：

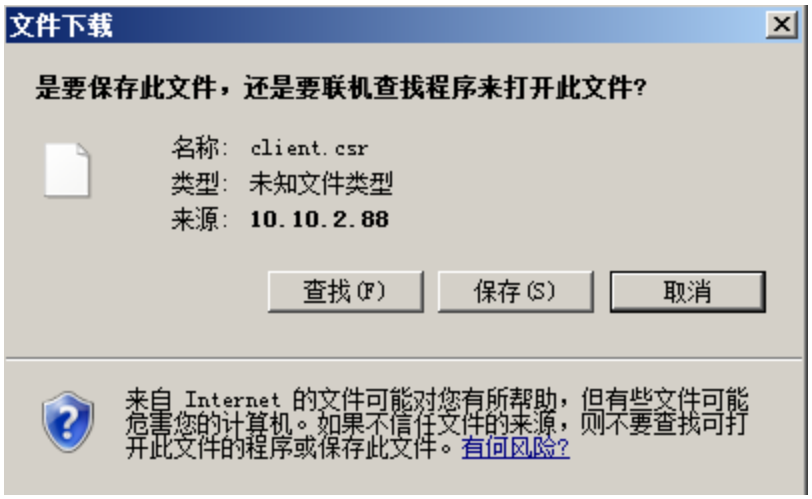


点击创建证书请求按钮，出现如下对话框：

此时填入'CN'-国家，'GD'-省份，'SZ'-城市，'SANGFOR'-公司，'SUPPORT'-部门，'www.sangfor.com.cn'-颁发对象，'support@sangfor.com.cn' - email 地址。每个字段都有限制（例如国家限制 2 位，省份限制 20 位），超出限制长度将不能再输入，且有可能报错（尽量使用英文字母）。配置完成后，点击确定。



点击下载保存，如图：

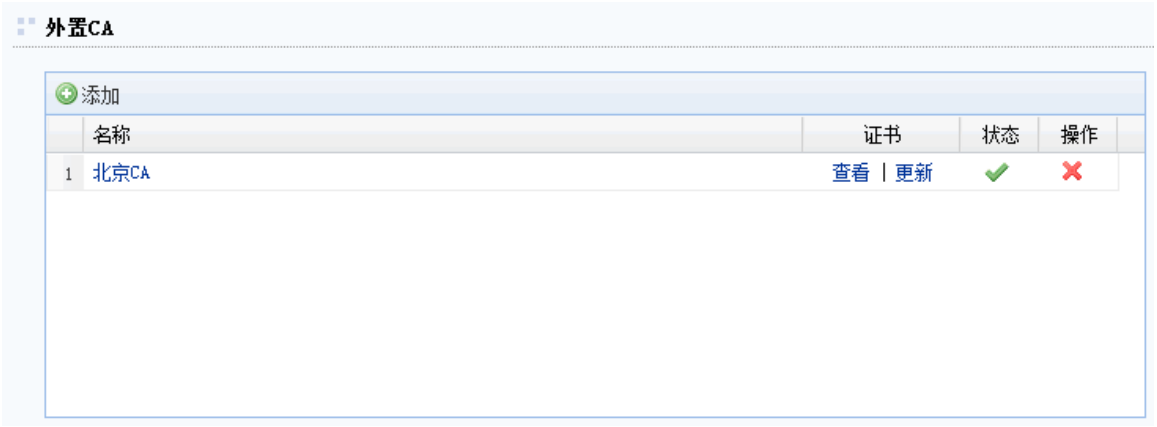


打开 client.csr 后显示如下：

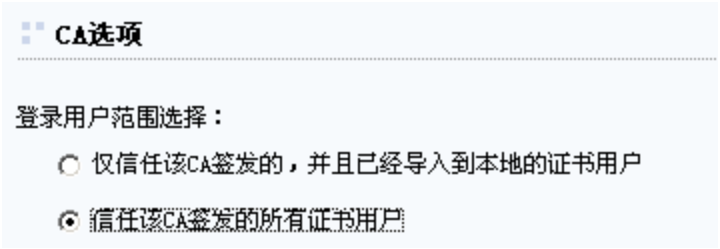
第二步：将完整代码全部复制到一个文本文档中，将生成的第三方证书请求提交给第三方 CA 认证机构。

第三步：从第三方 CA 认证机构拿到 CA 根证书和用户证书；

第四步：进入『VDI 设置』→『认证设置』→『证书与 USB-KEY 认证』页面，在『外置 CA』中，点击添加按钮，将获取的 CA 根证书导入设备；



第五步：点击外置 CA 名称，设置信任该 CA 签发的所有证书用户，如下图所示：



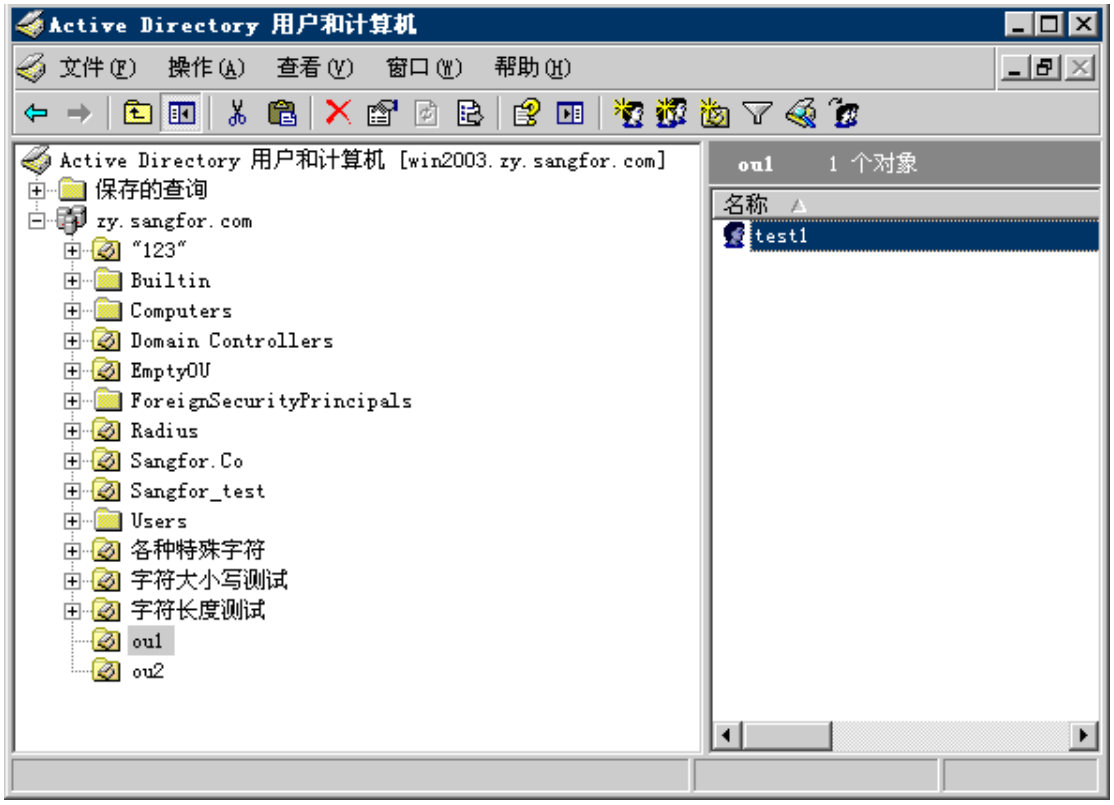
第六步：此时，用户即可以使用第三方 CA 颁发的证书登录 VDI 了。

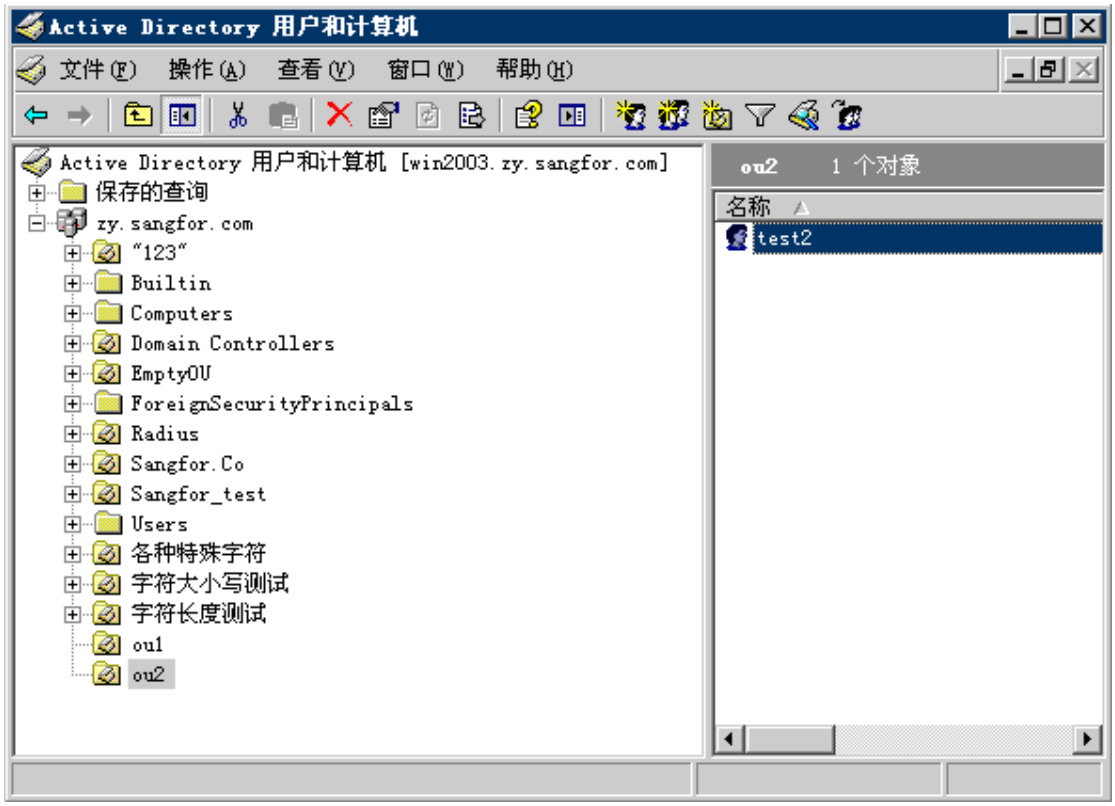
8.7.2. CA 中心映射规则配置案例

案例目标：结合第三方 CA 实现证书认证，并且保证某些用户登录进来之后自动分配到相应的用户组，拥有该用户组的权限。

以微软 CA 为例，微软 CA 颁发用户证书，用户都是存在域 MS LDAP 中的，例如：ldap 中各个用户的权限各不相同，客户希望不同 OU 下的用户登录到 VDI 之后也拥有不同权限，并且客户通过 CA 中心已经为这些需要认证的用户生成证书，希望这些用户登录 VDI 时能通过第三方证书认证。

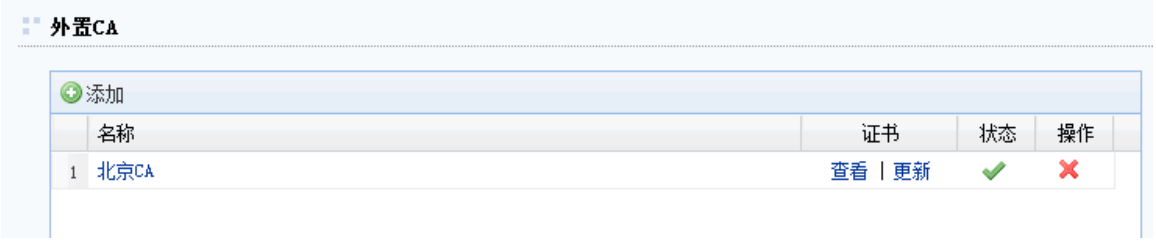
具体需求：LDAP 中有不同的 OU，要实现不同的 OU 下的用户通过第三方证书认证之后自动分配到不同的权限。如下图，test1 隶属于 ou1，test2 隶属于 ou2，要实现两个用户登录 VDI 后自动分配不同的资源，并且不需要把 test1 和 test2 两个用户导入到设备中。


Active Directory 用户和计算机
文件(F) 操作(A) 查看(V) 窗口(W) 帮助(H)
Active Directory 用户和计算机 [win2003.zy.sangfor.com]
保存的查询
zy.sangfor.com
"123"
Builtin
Computers
Domain Controllers
EmptyOU
ForeignSecurityPrincipals
Radius
Sangfor.Co
Sangfor_test
Users
各种特殊字符
字符大小写测试
字符长度测试
ou1
ou2
ou1 1 个对象
名称
test1

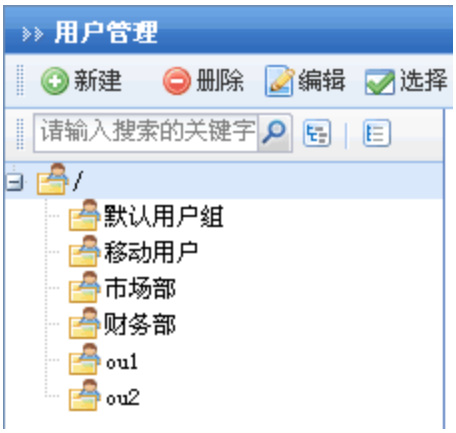

Active Directory 用户和计算机
文件(F) 操作(A) 查看(V) 窗口(W) 帮助(H)
Active Directory 用户和计算机 [win2003.zy.sangfor.com]
保存的查询
zy.sangfor.com
"123"
Builtin
Computers
Domain Controllers
EmptyOU
ForeignSecurityPrincipals
Radius
Sangfor.Co
Sangfor_test
Users
各种特殊字符
字符大小写测试
字符长度测试
ou1
ou2
ou2 1 个对象
名称
test2

配置步骤如下：

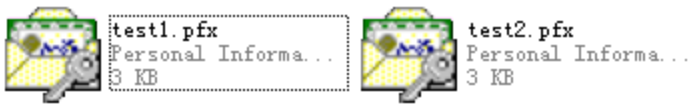
第一步：将设备设置为外部 CA 认证（具体配置参见 8.7 章节的案例配置过程）。



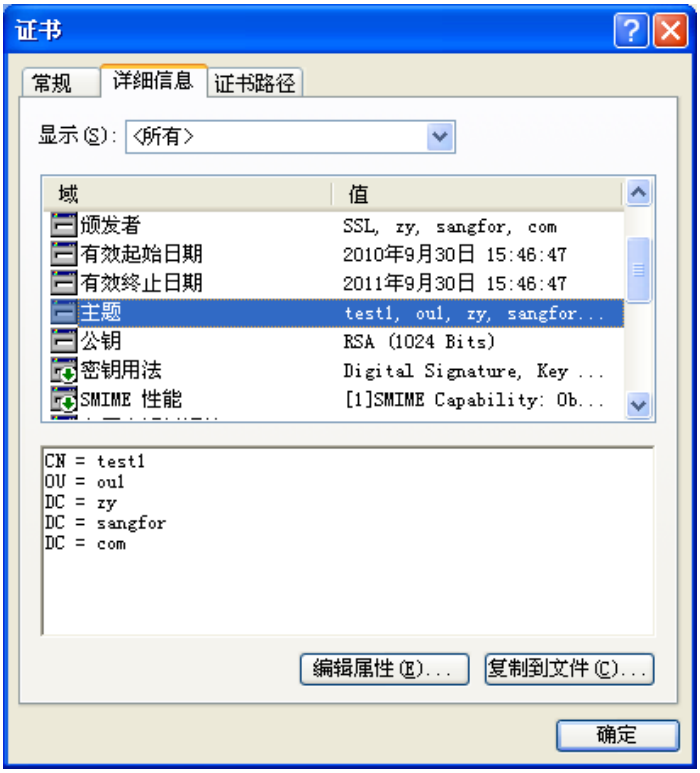
第二步：进入『VDI 设置』→『用户管理』页面，点击新建按钮，新增用户组，在 VDI 设备中新建两个用户组 ou1 和 ou2（新建过程此处不做详解），ou1 和 ou2 认证属性不需要设置证书认证：

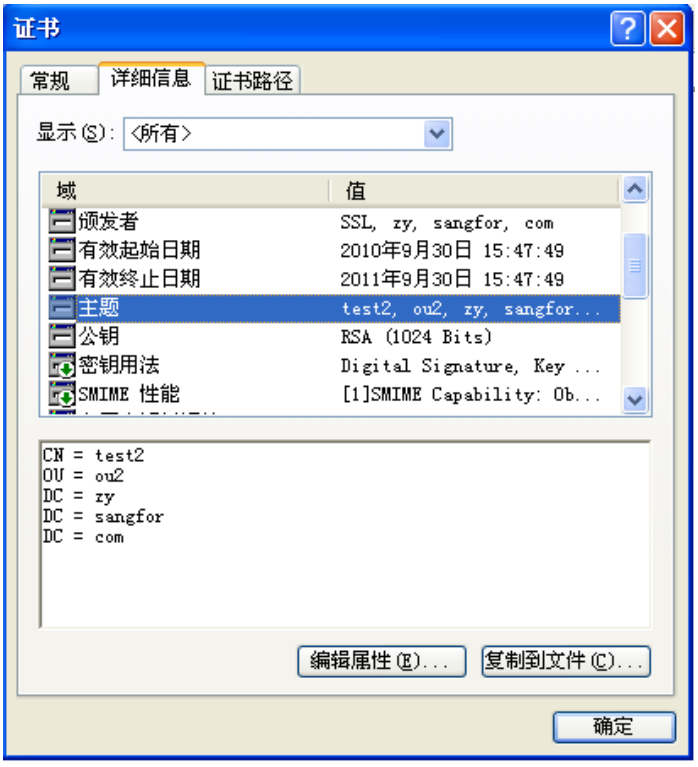


第三步：在 CA 中心分别为用户 test1、test2 申请用户证书：

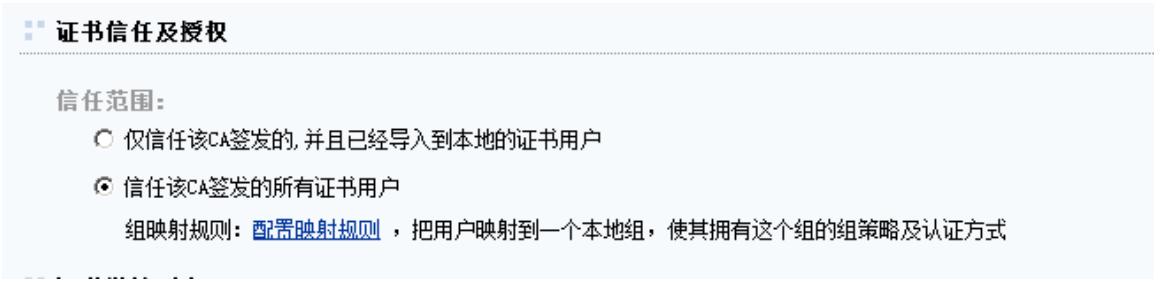


查看两个证书的主题项可知，test1 的 DN 是：CN=test1，OU=ou1，DC=zy，DC=sangfor，DC=com；test2 的 DN 是：CN=test2，OU=ou2，DC=zy，DC=sangfor，DC=com：

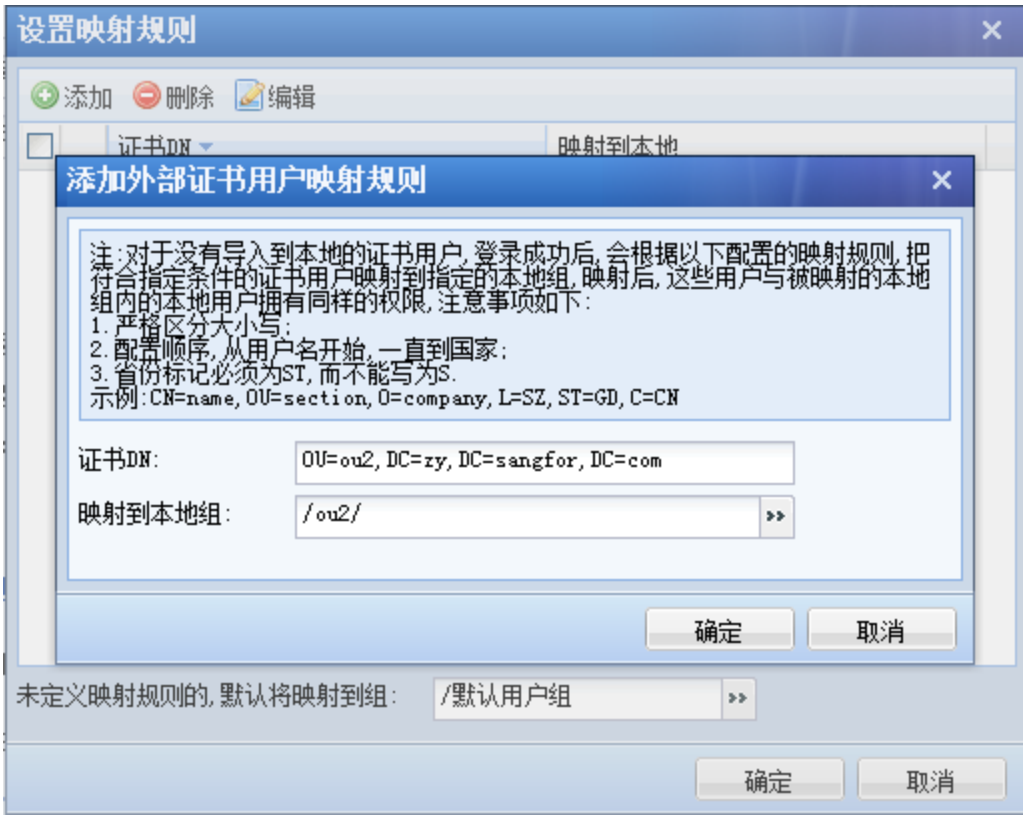




第四步：设置 CA 中心组映射规则，选择『信任该 CA 签发的所有证书用户』：



点击配置映射规则中，添加并设置 LDAP 中 ou1 映射为 VDI 中的 ou1 组，LDAP 中 ou2 映射为 VDI 中的 ou2 组：



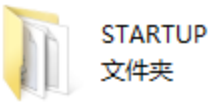
第五步：进入『VDI 设置』→『角色授权』页面，分别给 ou1 和 ou2 两个组分配不同的资源。

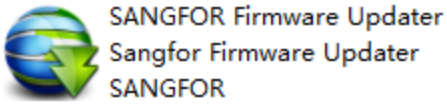
第六步：用户 test1 登录之后，分配到授权给 ou1 的资源。用户 test2 登录之后，分配到授权给 ou2 的资源。

附录一：SANGFOR 设备升级系统的使用

SANGFOR 设备升级系统可用于对设备进行内核版本升级和备份恢复设备配置。在设备出现致命错误时，也可通过 SANGFOR 设备升级系统把设备恢复到出厂状态。同时，SANGFOR 设备升级系统还可以启动技术支持工具来检查系统网口工作状态，路由等配置信息以及更改网口工作模式等。

SANGFOR 设备升级系统为绿色版软件，解压后即可使用，解压文件里包含一个文件夹和一个主程序，界面如下：





双击打开主程序的主界面，界面如下：

『设备 IP 地址』：连接的 SANGFOR VDC 设备的 IP 地址，格式为 IP：端口，也可以直接输入 IP 地址进行访问，则默认连接的是该 IP 地址的 51111 端口。

『管理员密码』：为 VDC 设备控制台超级管理员 admin 账号对应的密码。

『查找设备』：通过点击查找设备来搜索局域网内部的 SANGFOR 设备。

输入 SANGFOR 设备的 IP 地址以及管理员密码后，点击连接即可连接到设备进行系统升级、恢复默认配置等操作，界面如下：

『当前设备信息』：用于显示连接的 SANGFOR 设备的版本信息以及连接的 IP 地址。

『设备升级』：对当前连接的 SANGFOR 设备进行升级操作，包括在线升级和从本地加载升级包进行升级。

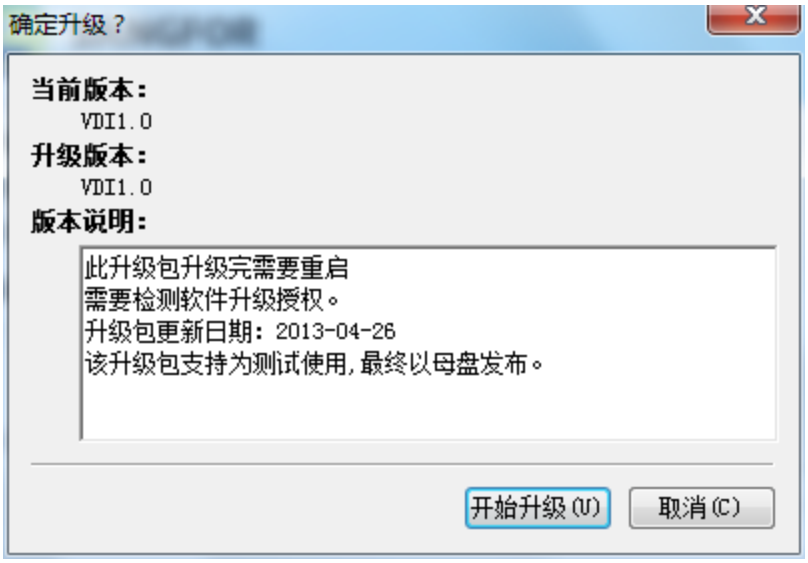
在线升级：

选择在线升级，点击选择版本，SANGFOR 设备升级系统会自动判定设备当前版本支持升级到哪个版本，并自动列出可以支持升级的版本信息，选择期望升级到的版本，点击确定后，系统会自动从服务器上下载升级包进行升级操作。

使用 SANGFOR 设备升级系统进行在线升级时，要求所连接的 SANGFOR 设备能够正常上网，否则将不能进行在线升级。

从本地加载升级包：

选择从本地加载升级包，点击浏览，选择下载到本地的相应升级包，然后点击下一步，显示当前升级包的基本信息，确认无误后，点击开始升级进行升级操作，界面如下：



升级完成后，设备升级状态里会显示“升级成功”。

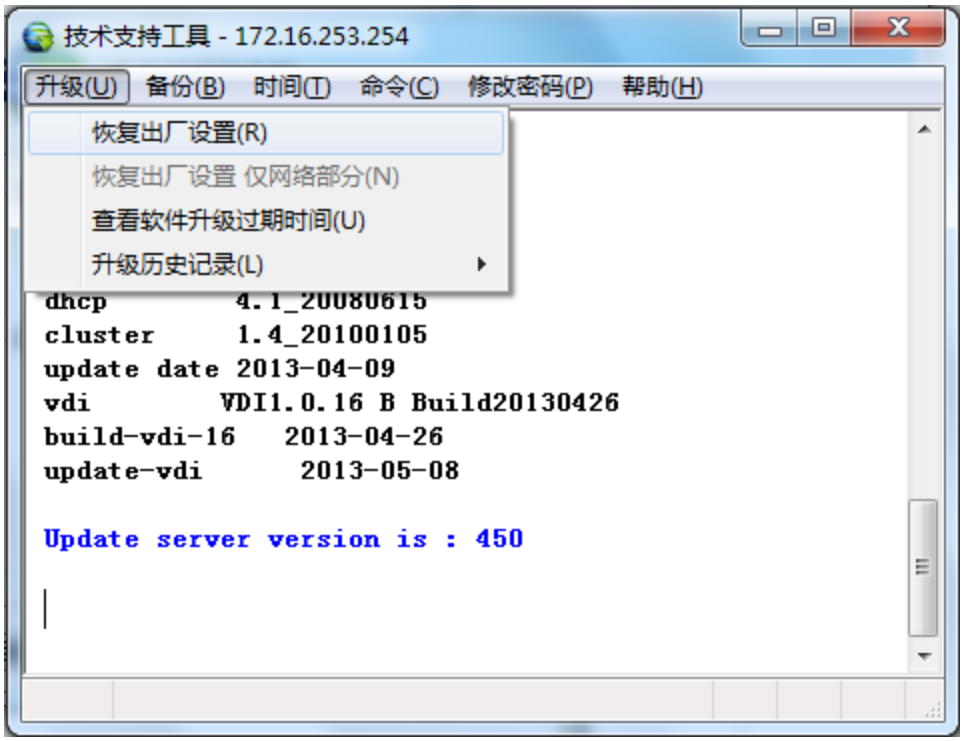
1．设备只能从低版本升级到高版本，而且一般不能跨版本升级。

2．升级具有一定的风险，如升级不当会导致设备损坏。请勿自行升级。如需升级请联系深信服科技客户服务部。

启动技术支持工具：

SANGFOR 设备升级系统连接到 SANGFOR 设备后，可以按 F10 或 Ctrl+Shift+F10 启动技术支持工具。技术支持工具有『升级』、『备份』、『时间』、『命令』、『修改密码』和『帮助』几个菜单，下面分别介绍它们的功能。

『升级』：包括恢复出厂设置，恢复出厂设置仅网络部分，查看软件升级过期时间和升级历史记录。如下图：



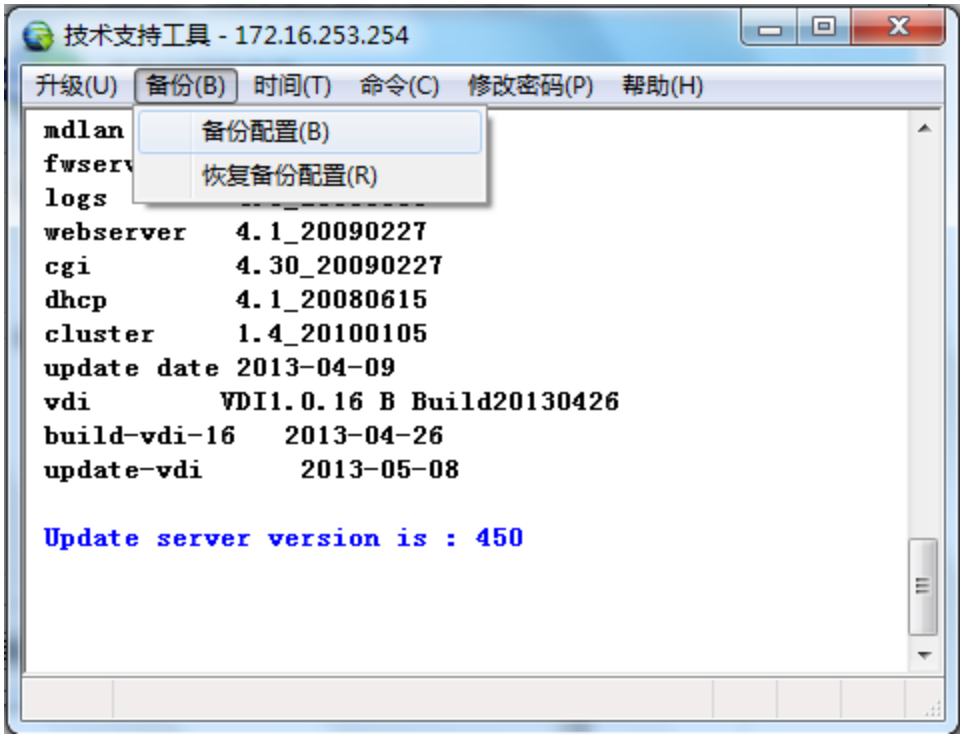
[恢复出厂设置]：用于将 SANGFOR 硬件设备恢复到默认配置，需要通过加载升级包将设备恢复出厂设置。

[恢复出厂设置仅网络部分]：只能在没有连接到设备时才能使用。会将设备的网络配置恢复到默认出厂配置，此操作是通过广播包发送命令进行操作的，会对局域网内的所有 SANGFOR 硬件网关生效，有一定危险性，请勿擅自点击操作。

[查看软件升级过期时间]：检测当前网关是否处于升级服务有效期内。若不在升级服务有效期内，则不能升级，需要购买相应授权才能升级。

[升级历史记录]：用于查看当前设备的以往升级历史，或者查看或清除本地的历史升级记录。

『备份』：包括备份配置、恢复备份配置选项，如下图：

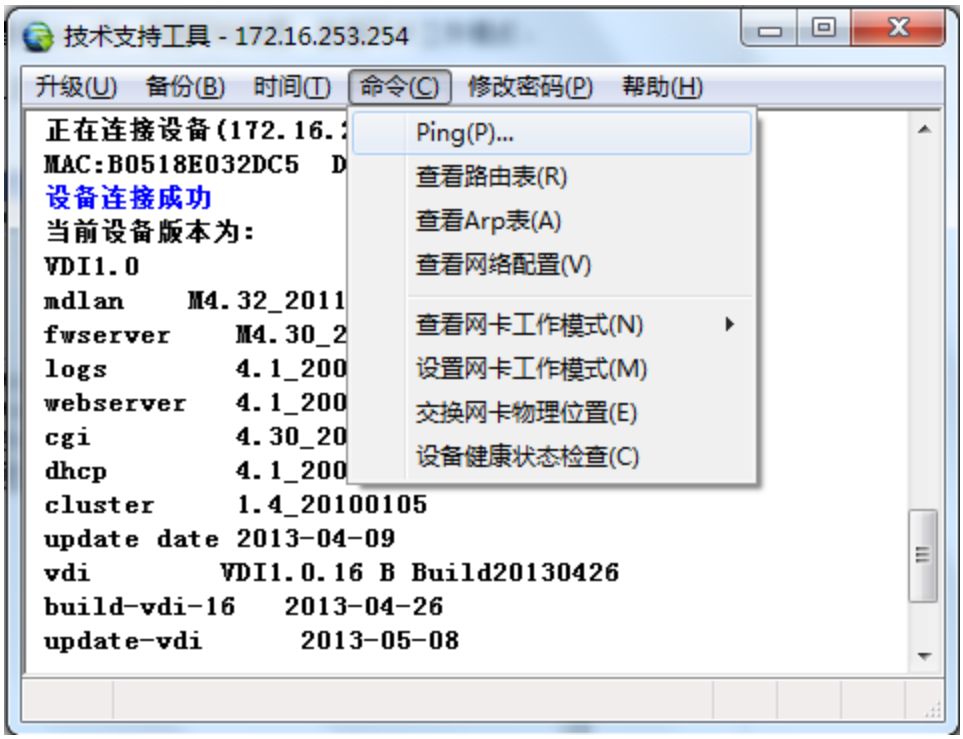


[备份配置]：将设备现有的配置信息进行备份。

[恢复备份配置]：将以前备份过的配置信息恢复到设备中。

『时间』用来查看当前时间和同步公网时间，来效验设备升级授权是否过期。

『命令』：包括 Ping、查看路由表、查看 Arp 表、查看网络配置、查看网卡工作模式、设置网卡工作模式、交换网卡物理位置以及设备健康状态检查选项。如下图：



[Ping]：登录设备后，从设备往外网 ping，以验证设备是否和外网连通。

[查看路由表]：查看设备本机的路由表。

[查看 Arp 表]：查看设备本机的 ARP 表。

[查看网络配置]：查看设备本机的网络配置，包括接口 IP 配置等。

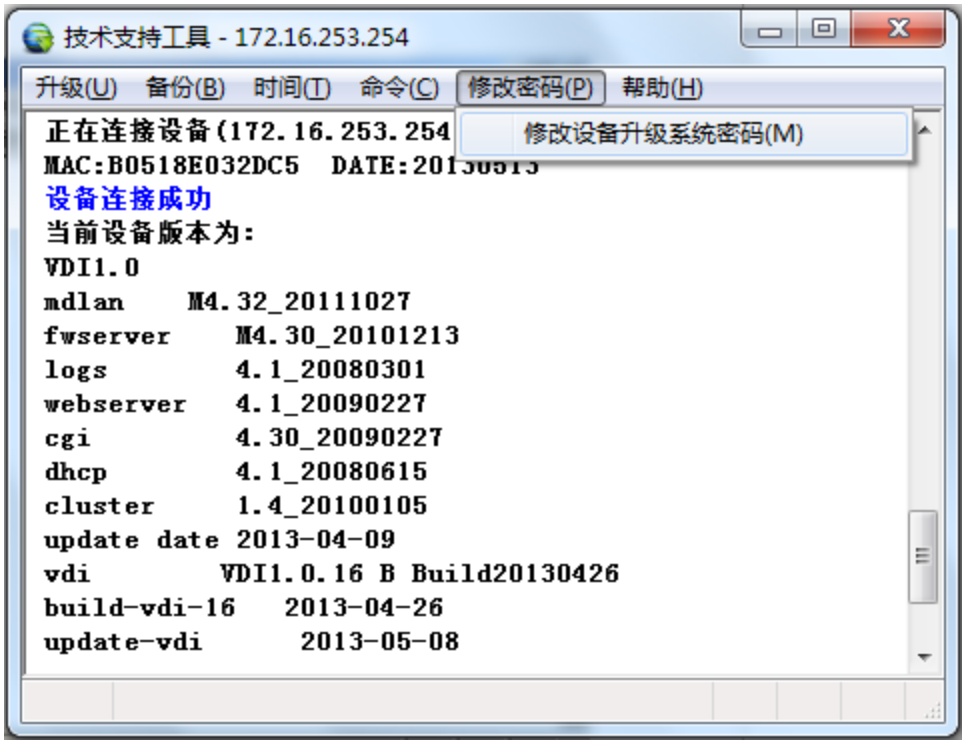
[查看网卡工作模式]：查看设备各网卡的工作模式。

[设置网卡工作模式]：设置指定网卡的工作模式。

[交换网卡物理位置]：用于交换网卡的物理位置。

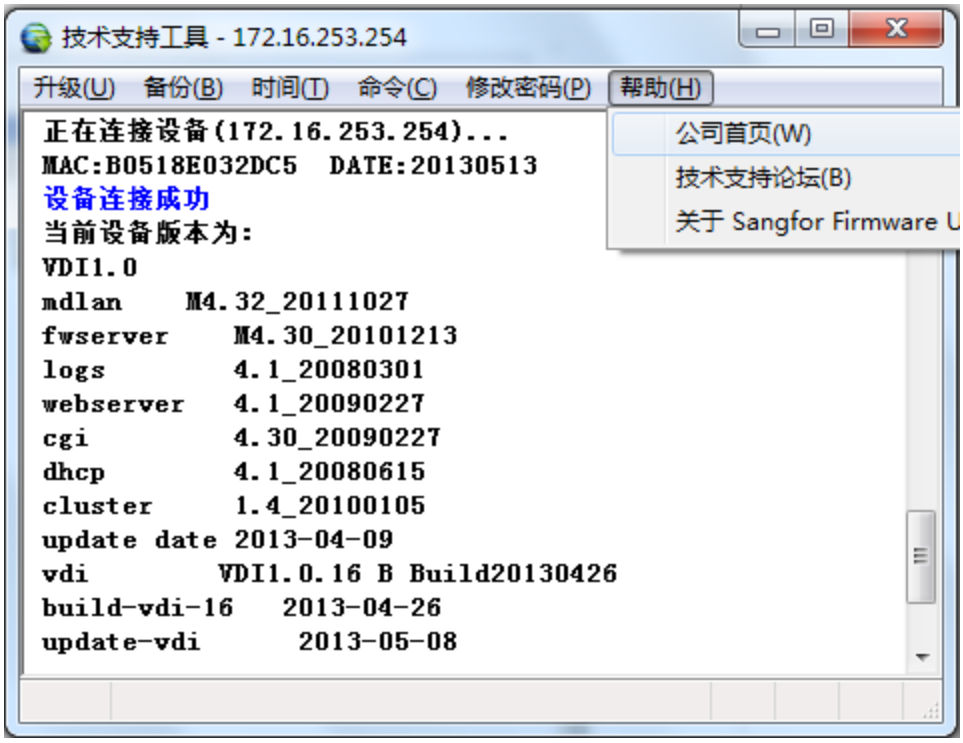
[设备健康状态检查]：通过在线检测或者是上传脚本来检测设备的硬件状态。

『修改密码』：用于修改 SANGFOR 设备升级系统密码。



SANGFOR 设备升级系统的密码为 VDC 设备控制台超级管理员 admin 账号对应的密码，所以此处的修改密码选项对 VDC 设备无效。

『帮助』包括公网首页的链接，技术支持论坛的链接和查看当前 Updater 的版本信息。


技术支持工具 - 172.16.253.254
升级(U) 备份(B) 时间(T) 命令(C) 修改密码(P) 帮助(H)
公司首页(W)
技术支持论坛(B)
关于 Sangfor Firmware U
正在连接设备(172.16.253.254)...
MAC:B0518E032DC5 DATE:20130513
设备连接成功
当前设备版本为:
VDI1.0
mdlan M4.32_20111027
fwserver M4.30_20101213
logs 4.1_20080301
webserver 4.1_20090227
cgi 4.30_20090227
dhcp 4.1_20080615
cluster 1.4_20100105
update date 2013-04-09
vdi VDI1.0.16 B Build20130426
build-vdi-16 2013-04-26
update-vdi 2013-05-08

附录二：使用 U 盘恢复网络配置和密码

SANGFOR VDC 设备支持使用 U 盘恢复网络配置和密码。在 U 盘里分别放入对应功能名称的 txt 文件，通过将 U 盘插入设备的 USB 口来实现恢复功能。

功能 1：使用 U 盘恢复设备网络配置。

功能 2：使用 U 盘查看网口配置。

功能 3：使用 U 盘恢复控制台密码。

使用 U 盘恢复网络配置

1、将 reset-network.txt 文件拷贝到 U 盘根目录；

2、插入 U 盘，重启设备；

3、当设备的 LED 红灯熄灭之后，拔出 U 盘；

4、查看 U 盘中的结果文件 reset-network.log，若恢复成功则在该文件中可以看到恢复后的网络配置，否则其中记录的是恢复失败信息；

5、重启设备以使新的网络配置生效。

使用 U 盘查看网口配置

1、将 show-ifconfig.txt 文件拷贝到 U 盘根目录；

2、插入 U 盘，重启设备；

3、当设备的 LED 红灯熄灭之后，拔出 U 盘；

4、 查看 U 盘中的结果文件 show-ifconfig.log，可知当前的网口配置。

使用 U 盘恢复控制台密码

1、将 reset-password.txt 文件拷贝到 U 盘根目录；

2、插入 U 盘，重启设备；

3、当设备的 LED 红灯熄灭之后，拔出 U 盘；

4、查看 U 盘中的结果文件 reset-password.log，若恢复成功在该文件中记录恢复后的控制台密码，否则记录的是恢复失败信息。

注意事项

1、这三个 txt 文件可以直接在 windows 系统上建立空白 txt 文件，将文件名字改成对应功能要求的文件名即可；

2、txt 文件必须在 U 盘的根目录下；

3、U 盘可以为单分区或多分区。单分区的 U 盘格式必须为 FAT32；多分区 U 盘必须把 txt 文件放在第一个分区，且第一个分区格式必须为 FAT32；

4、以上三个功能不互斥，一次可以同时进行多个操作。