UNIS A2000-G 系列运维审计系统

典型配置举例

北京紫光恒越网络科技有限公司
http://www.unishy.com

资料版本：5W100-20180521

前 言

本配置指导介绍了 UNIS A2000-G 系列运维审计系统的常用典型配置举例及其配置步骤。

前言部分包含如下内容：

读者对象

本手册主要适用于如下工程师：

- 网络规划人员
- 现场技术支持与维护人员
- 负责网络配置和维护的网络管理员

本书约定

1. 命令行格式约定

格　式	意　义
粗体	命令行关键字（命令中保持不变、必须照输的部分）采用**加粗**字体表示。
斜体	命令行参数（命令中必须由实际值进行替代的部分）采用*斜体*表示。
[ ]	表示用“[ ]”括起来的部分在命令配置时是可选的。
{ x | y | ... }	表示从多个选项中仅选取一个。
[x | y | ...]	表示从多个选项中选取一个或者不选。
{ x | y | ... } *	表示从多个选项中至少选取一个。
[x | y | ...] *	表示从多个选项中选取一个、多个或者不选。
&<1-n>	表示符号&前面的参数可以重复输入1～n次。
#	由“#”号开始的行表示为注释行。

2. 图形界面格式约定

格　式	意　义
< >	带尖括号“< >”表示按钮名，如“单击<确定>按钮”。
[ ]	带方括号“[ ]”表示窗口名、菜单名和数据表，如“弹出[新建用户]窗口”。
/	多级菜单用“/”隔开。如[文件/新建/文件夹]多级菜单表示[文件]菜单下的[新建]子菜单下的[文件夹]菜单项。

3. 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：

 警告	该标志后的注释需给予格外关注，不当的操作可能会对人身造成伤害。
 注意	提醒操作中应注意的事项，不当的操作可能会导致数据丢失或者设备损坏。
 提示	为确保设备配置成功或者正常工作而需要特别关注的操作或信息。
 说明	对操作内容的描述进行必要的补充和说明。
 窍门	配置、操作、或使用设备的技巧、小窍门。

4. 图标约定

本书使用的图标及其含义如下：

	该图标及其相关描述文字代表一般网络设备，如路由器、交换机、防火墙等。
	该图标及其相关描述文字代表一般意义下的路由器，以及其他运行了路由协议的设备。
	该图标及其相关描述文字代表二、三层以太网交换机，以及运行了二层协议的设备。
	该图标及其相关描述文字代表无线控制器、无线控制器业务板和有线无线一体化交换机的无线控制引擎设备。
	该图标及其相关描述文字代表无线接入点设备。
	该图标及其相关描述文字代表无线终结单元。
	该图标及其相关描述文字代表无线终结者。
	该图标及其相关描述文字代表无线Mesh设备。
	该图标代表发散的无线射频信号。
	该图标代表点到点的无线射频信号。
	该图标及其相关描述文字代表防火墙、UTM、多业务安全网关、负载均衡等安全设备。
	该图标及其相关描述文字代表防火墙插卡、负载均衡插卡、NetStream插卡、SSL VPN插卡、IPS插卡、ACG插卡等安全插卡。

5. 端口编号示例约定

本手册中出现的端口编号仅作示例，并不代表设备上实际具有此编号的端口，实际使用中请以设备上存在的端口编号为准。

技术支持

用户支持邮箱：zgsm_service@thunis.com

技术支持热线电话：400-910-9998（手机、固话均可拨打）

网址：http://www.unishy.com

资料意见反馈

如果您在使用过程中发现产品资料的任何问题，可以通过以下方式反馈：

E-mail：zgsm_info@thunis.com

感谢您的反馈，让我们做得更好！

AD&LDAP 认证配置举例

目 录

1 简介

1. LDAP

LDAP 是轻量目录访问协议，英文全称是 Lightweight Directory Access Protocol，简称为 LDAP。目录服务是一种特殊的数据库系统，其专门针对读取，浏览和搜索操作进行了特定的优化。目录一般用来包含描述性的，基于属性的信息并支持精细复杂的过滤能力。目录一般不支持通用数据库针对大量更新操作操作需要的复杂的事务管理或回卷策略。而目录服务的更新则一般都非常简单。这种目录可以存储包括个人信息、web 链接、jpeg 图像等各种信息。为了访问存储在目录中的信息，就需要使用运行在 TCP/IP 之上的访问协议—LDAP。

2. AD

AD 是 Active Directory 的缩写，AD 应该是 LDAP 的一个应用实例。比如：windows 域控的用户、权限管理应该是微软公司使用 LDAP 存储了一些数据来解决域控这个具体问题，只是 AD 顺便还提供了用户接口，也可以利用 ActiveDirectory 当做 LDAP 服务器存放一些自己的东西而已。比如 LDAP 是关系型数据库，微软自己在库中建立了几个表，每个表都定义好了字段。显然这些表和字段都是根据微软自己的需求定制的，而不是 LDAP 协议的规定。然后微软将 LDAP 做了一些封装接口，用户可以利用这些接口写程序操作 LDAP，使得 ActiveDirectory 也成了一个 LDAP 服务器。

2 名词解释

1. 条目

条目，也叫记录项，是 LDAP 中最基本的颗粒，就像字典中的词条，或者是数据库中的记录。通常对 LDAP 的添加、删除、更改、检索都是以条目为基本对象的。

2. DN

每一个条目都有一个唯一的标识名，如 dn="cn=baby,ou=marketing,ou=people,dc=mydomain,dc=org"。通过 DN 的层次型语法结构，可以方便地表示出条目在 LDAP 树中的位置，通常用于检索。

3. Basedn

LDAP 目录树的最顶部就是根，也就是所谓的“Base DN"，如"dc=mydomain,dc=org"。

在运维审计系统的 BaseDN 是指，以当前的组织作为根，搜索当前组织的范围。

4. 属性

每个条目都可以有很多属性（Attribute），比如常见的人都有姓名、地址、电话等属性。每个属性都有名称及对应的值。

5. 用户Filter

运维审计系统的用户 Filter 是指，通过属性来过滤用户。

例如：(&(objectclass=person)(sAMAccountName=testuser))，代表过滤出 objectclass 为 person 并且 sAMAccountName 为 testuser 的用户。

6. Simple方法

Simple 需用绑定查询用户及口令，配置相对灵活复杂，几乎所有的目录服务器都支持该验证方法。

7. Digest-md5 方法

仅需要知道 ldap 服务器的 FQDN 和 IP 地址既可，不需要绑定用户名和密码，配置方法相对简单。

8. 查询用户

在域控中，具有查询权限的用户。

3 配置前提

1. Windows（AD）

- 准备 Windows 域控主机一台。
- 准备 Windows 域控主机的相关信息：IP 地址、端口、计算机全名、查询用户、查询用户密码、BaseDN、用户 Filter。
- 确保域控主机到运维审计系统的网络可达。

2. LDAP

- 准备 LDAP 服务器一台。
- 准备 LDAP 服务器的相关信息：IP 地址、端口、查询用户、查询用户密码、BaseDN、用户 Filter。
- 确保 LDAP 服务器到运维审计系统的网络可达。

3. AD/LDAP典型配置

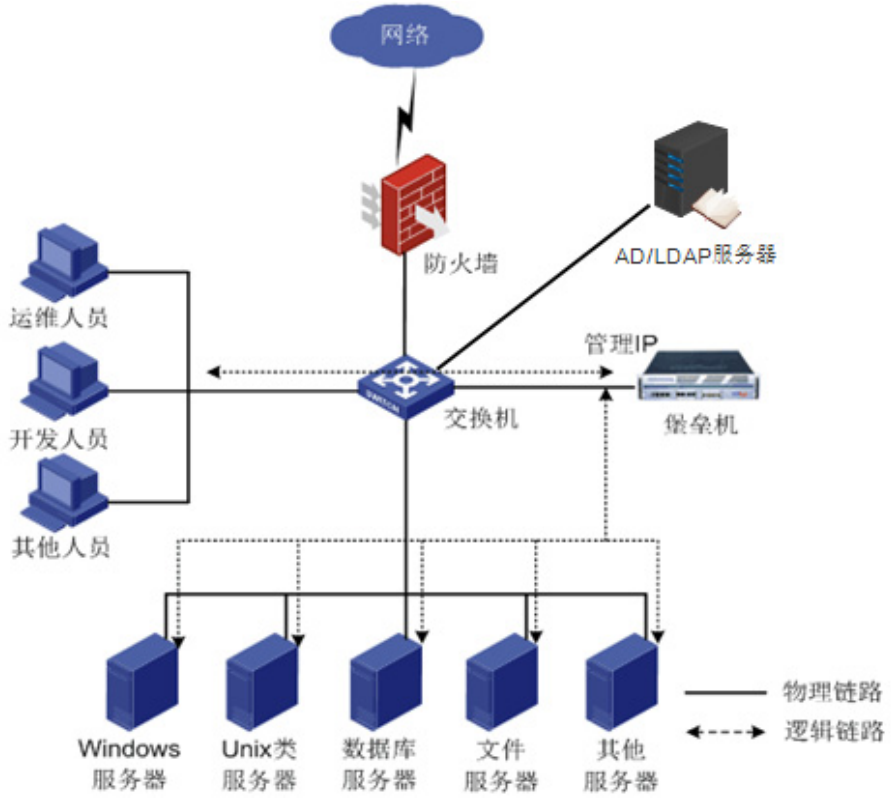
- DIGEST-MD5 设置：
  - 状态：启用服务器 1
  - 名称：Windows_AD
  - 方法：DIGEST-MD5
  - 服务器 1 全名：ad1.abc.com(AD（LDAP）服务器主机名全称)
  - 服务器 1 地址：192.168.6.200
  - 服务器 1 端口：389
  - 服务器 2 全名：ad2.abc.com
  - 服务器 2 地址：192.168.6.201
  - 服务器 2 端口：389
- SIMPLE 设置：
  - 状态：启用服务器 1
  - 名称：Windows_AD
  - 方法：SIMPLE
  - 服务器 1 地址：192.168.6.200
  - 服务器 1 端口：389
  - 服务器 2 地址：192.168.6.201
  - 服务器 2 端口：389
  - 查询用户 DN：CN=Administrator,CN=Users,DC=dep,DC=com
  - 查询用户密码：123456

- 用户 basedn：CN=Users,DC=dep,DC=com
- 用户 Filter：(&(objectclass=person)(sAMAccountName={username}))

4 配置举例

4.1 组网需求

图1 AD/LDAP 认证网络图



4.2 系统版本要求

适用产品版本：ESS 6102

4.3 Windows（AD） Digest-MD5认证

4.3.1 收集信息

- Windows 域控主机 IP 地址。
- Windows 域控主机的计算机全名。（控制面板\系统和安全\系统\计算机全名）
- Windows 域控主机 AD 服务的端口号。

4.3.2 配置步骤

1. 登录具有超级管理员角色的用户。

2. 创建ldap认证方式。

进入“策略配置 > 身份验证”，选择 ldap 协议，点击“创建”。

图2 创建 ldap 认证方式

3. 编辑ldap认证方式。

(1) 选择认证方法为“DIGEST-MD5”。

(2) 选择状态为：“启用服务器 1”。

(3) 填写“名称”、“服务器 1 全名”、“服务器 1 地址”、“服务器 1 端口”几个字段。

- 名称：填写此 AD 认证的名称。
- 服务器 1 地址：Windows 域控主机 IP 地址。
- 服务器 1 全名：Windows 域控主机的计算机全名。
- 服务器 1 端口：如果留空，默认为 389 端口。

(4) 点击“确定”，提交配置。

图3 配置 ldap 认证方式

4. 创建ldap用户。

进入“基本控制 > 用户账号”。点击“新建用户”。

图4 创建 ldap 用户

(1) 选择“身份验证方式”为刚才配置的名称。

(2) 填写“登录名”、“真实姓名”、“部门”、“ldap 用户名”这几个字段。

- 登录名：登录运维审计系统的账户名。
- 真实姓名：该账户名的真实用户。
- 部门：选择相应的部门。
- ldap 用户名：绑定该登录名对应的 ldap 账户，如果不填，则默认此项为登录名。

(3) 点击“保存”。

图5 配置 ldap 用户信息

5. 登录ldap用户。

图6 ldap 用户登录

4.3.3 验证配置

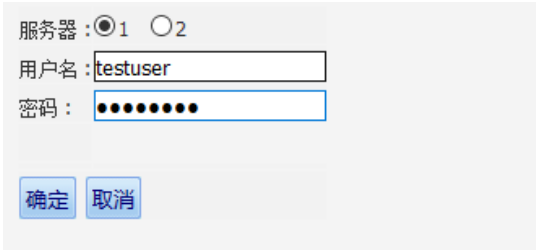
进入超级管理员账户。

(1) 选择“策略配置 > 身份验证”，选择相应的 ldap 认证，点击“测试”。

图7 身份验证

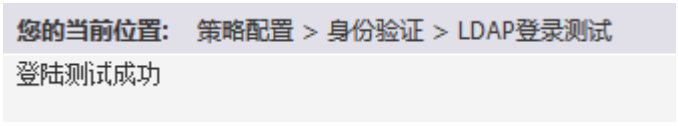
(2) 填写需要验证的账户密码，选择相应的服务器，点击“确定”。

图8 填写验证的账户密码



(3) 返回“登录测试成功”。

图9 登录成功



4.4 Windows（AD）simple认证

4.4.1 收集信息

- Windows 域控主机 IP 地址。
- Windows 域控主机 AD 服务的端口号。
- Windows 域控主机的查询用户的 DN（打开“cmd”，通过命令“dsquery user -name [username]”查询）。
- Windows 域控主机查询用户的密码。
- 用户 basedn（希望从哪一层组织下查找）。
- 用户 Filter（系统通过什么属性过滤用户）。

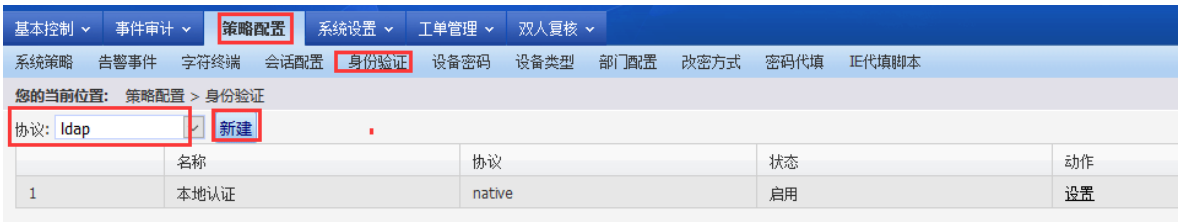
4.4.2 配置步骤

1. 登录具有超级管理员角色的用户。

2. 创建ldap认证方式。

进入“策略配置 > 身份验证”，选择 ldap 协议，点击“创建”。

图10 创建 ldap 认证方式



3. 编辑ldap认证方式。

(1) 选择认证方法为“SIMPLE”。

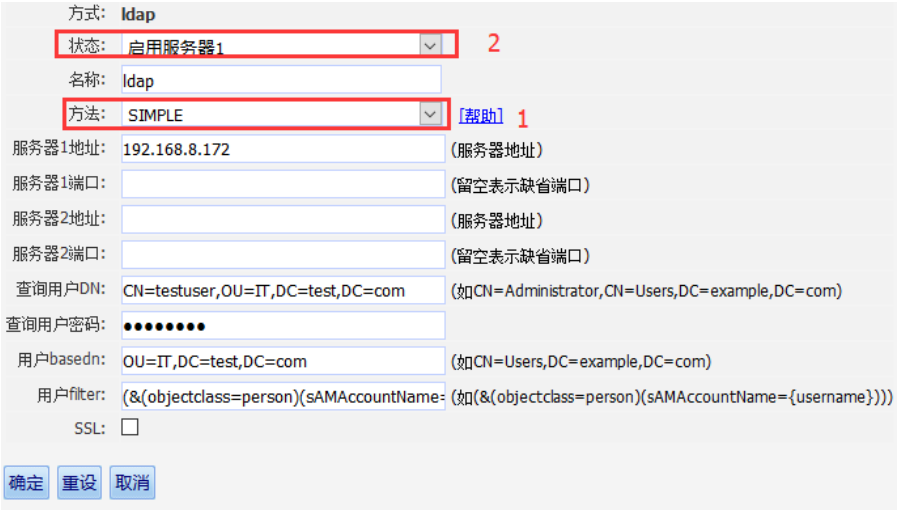
(2) 选择状态为：“启用服务器 1”。

(3) 填写“名称”、“服务器 1 地址”、“服务器 1 端口”、“查询用户 DN”、“查询用户密码”、“用户 BaseDN”、“用户 Filter”几个字段。

- 名称：填写此 ldap 认证的名称。
- 服务器 1 地址：Windows 域控主机 IP 地址。
- 服务器 1 端口：如果留空，默认为 389 端口。
- 查询用户 DN：具有查询权限的用户的 DN。
- 查询用户密码：查询用户密码。
- 用户 BaseDN：希望从那一层组织下查找。
- 用户 Filter：系统通过什么属性过滤用户。对于 windows 的域控可以通过“(&(objectclass=person)(sAMAccountName={username}))”过滤。其中{username}代表提交的变量，代表将来传入的用户名。

(4) 第 4 步：点击“确定”，提交配置。

图11 配置 ldap 认证方式



4. 创建ldap用户。

进入“基本控制 > 用户账号”。点击“新建用户”。

图12 创建 ldap 用户

(1) 选择“身份验证方式”为刚才配置的名称。

(2) 填写“登录名”、“真实姓名”、“部门”、“ldap 用户名”这几个字段。

- 登录名：登录运维审计系统的账户名。
- 真实姓名：该账户名的真实用户。
- 部门：选择相应的部门。
- ldap 用户名：绑定该登录名对应的 ldap 账户，如果不填，则默认此项为登录名。

(3) 点击“保存”。

图13 配置 ldap 用户

5. 登录ldap用户。

图14 ldap 用户登录

4.4.3 验证配置

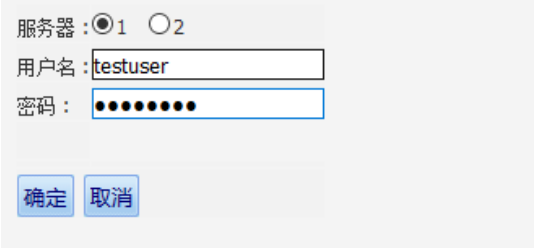
进入超级管理员账户。

(1) 选择“策略配置 > 身份验证”，选择相应的 ldap 认证，点击“测试”。

图15 身份验证

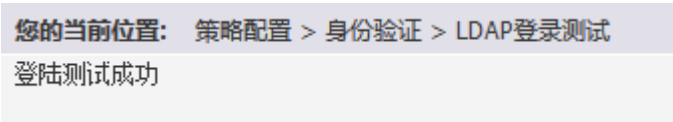
(2) 填写需要验证的账户密码，选择相应的服务器，点击“确定”。

图16 配置账户密码



(3) 返回“登录测试成功”。

图17 登录成功



4.5 Ldap simple认证

4.5.1 收集信息

- Ldap 服务器的 IP 地址。
- Ldap 服务器的 ldap 服务的端口号。
- Ldap 服务器的的查询用户的 DN。
- Ldap 服务器的查询用户的密码。
- 用户 basedn。（希望从那一层组织下查找）。
- 用户 filter。（系统通过什么属性过滤用户）。

4.5.2 配置步骤

1. 登录具有超级管理员角色的用户。

2. 创建ldap认证方式。

进入“策略配置 > 身份验证”，选择 ldap 协议，点击“创建”。

图18 创建 ldap 认证方式

3. 编辑ldap认证方式。

(1) 选择认证方法为“SIMPLE”。

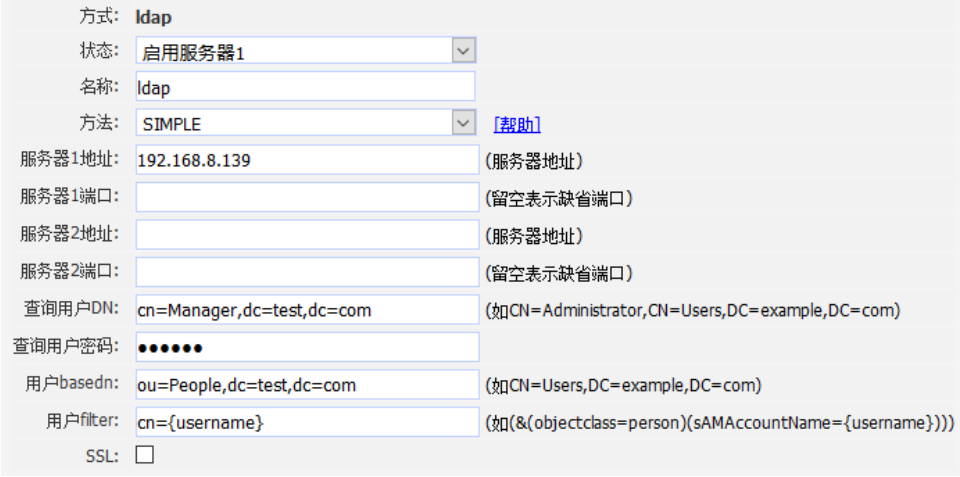
(2) 选择状态为：“启用服务器 1”。

(3) 填写“名称”、“服务器 1 地址”、“服务器 1 端口”、“查询用户 DN”、“查询用户密码”、“用户 BaseDN”、“用户 Filter”几个字段。

- 名称：填写此 ldap 认证的名称。
- 服务器 1 地址：Ldap 服务器的 IP 地址。
- 服务器 1 端口：如果留空，默认为 389 端口。
- 查询用户 DN：具有查询权限的用户的 DN。
- 查询用户密码：查询用户密码。
- 用户 BaseDN：希望从那一层组织下查找。
- 用户 Filter：系统通过什么属性过滤用户。这里通过 cn 属性可以过滤出用户，所以使用 cn={username}。

(4) 点击“确定”，提交配置。

图19 配置 ldap 认证方式



4. 创建ldap用户。

进入“基本控制 > 用户账号”。点击“新建用户”。

图20 创建 ldap 用户

(1) 选择“身份验证方式”为刚才配置的名称。

(2) 填写“登录名”、“真实姓名”、“部门”、“ldap 用户名”这几个字段。

- 登录名：登录运维审计系统的账户名。
- 真实姓名：该账户名的真实用户。
- 部门：选择相应的部门。
- ldap 用户名：绑定该登录名对应的 ldap 账户，如果不填，则默认此项为登录名。

(3) 点击“保存”。

图21 配置 ldap 用户信息

5. 登录ldap用户。

图22 Ldap 用户登录

4.5.3 验证配置

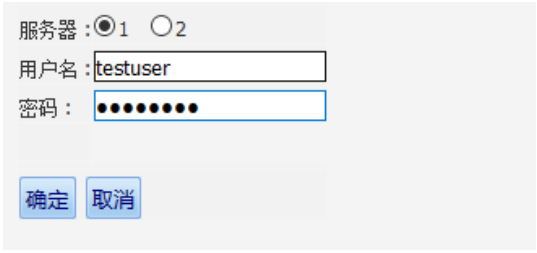
进入超级管理员账户。

(1) 选择“策略配置 > 身份验证”，选择相应的 ldap 认证，点击“测试”。

图23 身份验证

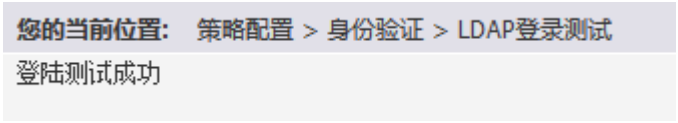
(2) 填写需要验证的账户密码，选择相应的服务器，点击“确定”。

图24 配置账户密码



(3) 返回“登录测试成功”。

图25 登录成功



4.6 Ldap用户批量导入

Ldap 用户的批量导入功能，仅限 simple 配置的方法。

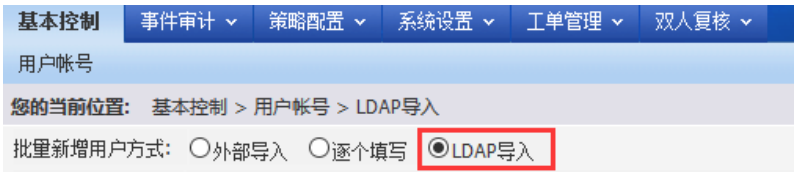
4.6.1 新建批量导入

(1) “基本控制 > 用户账号 > 批量导入”。

图26 批量导入

(2) “批量新增用户方式”选择“LDAP 导入”。

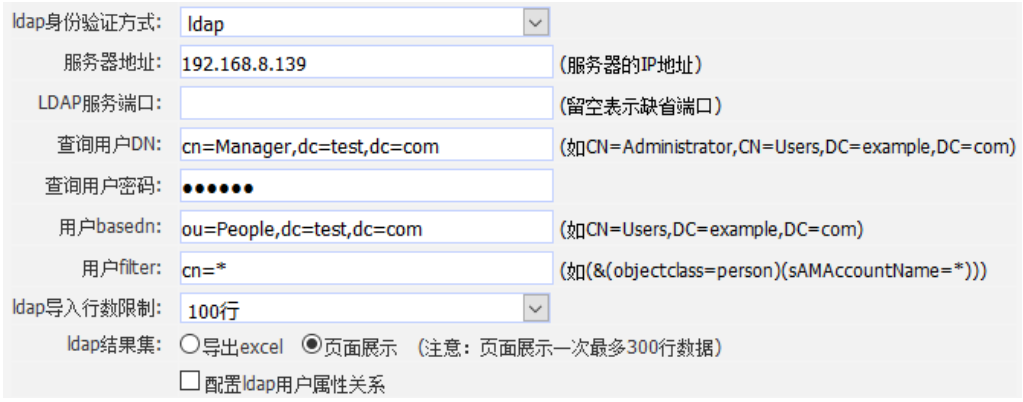
图27 配置批量新增用户方式



4.6.2 编辑批量导入规则

- Ldap 身份验证方式：选择之前配置的 ldap 的名称。
- 服务器地址：填写需要从哪一个 ldap 服务器进行导入。
- LDAP 服务端口：如果不填写，默认为 389 端口。
- 查询用户 DN：具有查询权限的用户的 DN。
- 查询用户密码
- 用户 basedn：希望从那一层组织下导入。
- 用户 filter：系统通过什么属性过滤用户。这里通过 cn 属性可以过滤出用户，所以使用 cn=*。

图28 编辑批量导入规则



如果需要将 ldap 上的用户属性也导入运维审计系统，可以在这里设置。

图29 配置 ldap 上的用户属性

4.6.3 提交批量导入规则

运维审计系统会将查询到的用户以表格的方式列出。

如果确认无误，点击“确定”，创建用户。

图30 提交批量导入规则

HA 部署配置举例

目 录

1 简介

本文档介绍两台运维审计系统的双机热备模式，实现运维审计系统的系统配置定期同步，提供运维审计系统的高可用性。

2 配置前提

本文档不严格与具体软、硬件版本对应，如果使用过程中与产品实际情况有差异，请以设备实际情况为准。

本文档中的配置均是在实验室环境下进行的配置和验证，配置前设备的所有参数均采用出厂时的缺省配置。如果您已经对设备进行了配置，为了保证配置效果，请确认现有配置和以下举例中的配置不冲突。

本文档假设您已了解 HA 特性。

3 使用限制

- 必须是安装相同软件版本的两台相同硬件设备。
- 必须使用业务数据口作为管理口。
- 业务数据口需要属于同一网段。
- 两台机器心跳口需用网线直连。

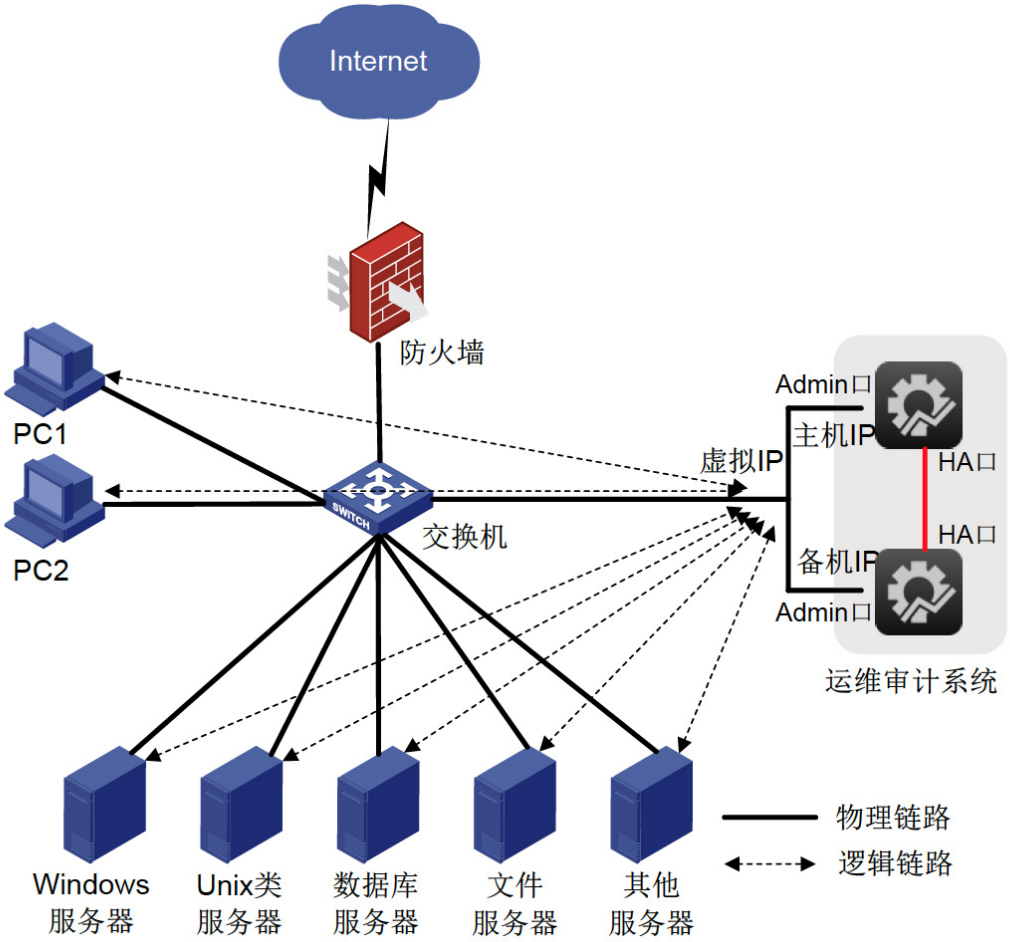
4 HA部署配置举例

4.1 组网需求

为了解决单点故障问题，运维审计系统采用双机热备模式，使用虚 IP 对外提供服务。当一台主机出现问题后，服务自动切换到另外一台机器继续提供服务。具体应用如下：

- 正常情况下，用户访问虚 IP 登录运维审计系统。
- 配置 NTP 服务器，保证时间同步。
- 当主机出现故障后，备机自动接管服务，虚 IP 浮动到备机。
- 当主机恢复故障后，服务依旧在备机继续提供服务。
- 当备机出现故障后，则切换方式相同。
- 运维审计系统与被管理设备之间路由可达、协议可通。
- PC 端只可访问运维审计系统虚 IP 的 22、443、3389 与 5899 端口。

图1 HA 部署组网图



4.2 系统版本要求

适用产品版本：ESS 6102

4.3 配置思路

- 分别配置两台运维审计系统的网络接口 IP 地址，必须在同一网段。
- 分别配置两台运维审计系统的 HA 接口 IP 地址，并且直连。
- 选取其中一台作为主机，编写配置 HA 信息，启动主机 HA 服务。
- 在另外一台机器上，配置 HA 信息，启动 HA 服务并加入到 HA 中。
- 配置完成后，两台机器即为双机热备的工作模式。

4.4 配置注意事项

为了确保双机热备配置成功，需要注意以下几方面：

- 两台运维审计系统的软件版本必须相同。
- 主机与备机的网络接口 IP 地址需在同一网段。
- 主机与备机 HA 接口 IP 必须直连并互通。
- 先配置主机，服务正常启动后在配置备机。

4.5 配置步骤

4.5.1 登录Main menu菜单

通过连接键盘、显示器到物理机登录 Main menu 菜单，用户名密码为 root/admin。
通过 SSH 远程连接登录 Main menu 菜单，使用密钥进行加密认证。

提示

密钥为登陆运维审计系统后台管理菜单的唯一认证方式。

运维审计系统的密钥内容如下：

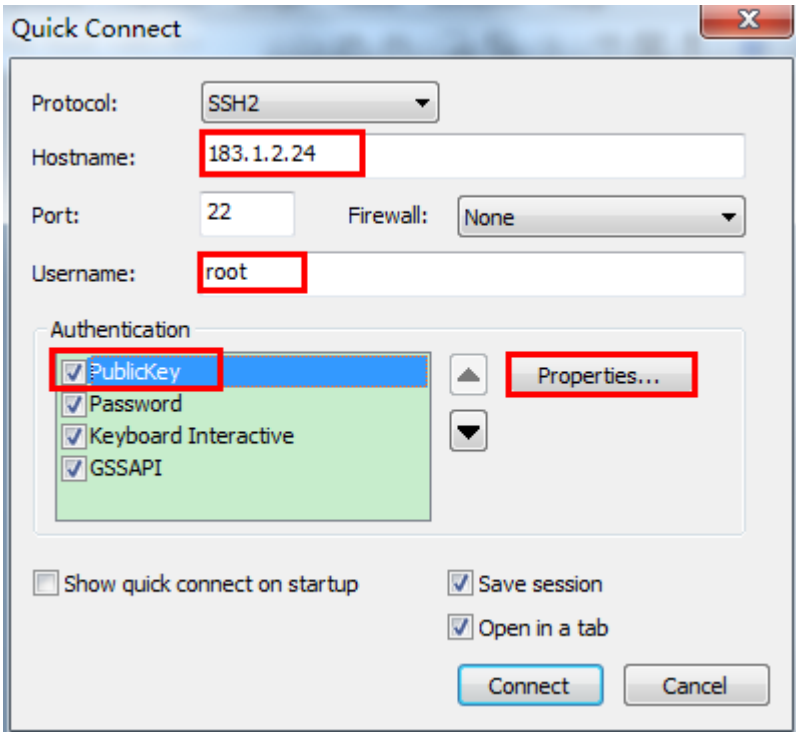
```
-----BEGIN RSA PRIVATE KEY-----
MIIEogIBAAKCAQEA7JSUgUq+1L9AlvK+6TRCN4mBTSVszAEu6llYhMOFcqM0I4o4
74ZaqWwi/JDwLnpi4HnW7h6OlM39I9qeKv1o9qbGUaXdgL+IkcJB4PVgCgeQKGlZ
B3ng/iOFe47dTV6Dx3D5v3j7lxuihPJXwcHtRRjSD0GBH0IJeQAL2fK3rk4ldqhI
FouqgoyjdONrV0YInRdNWzpl2Nxob33B/U4pwdvKVqDzWDk17+tZEdFvaoqzXFgt
hGfnmDtNiGVSLrJjbH+lwN0JHVeUSZHQ0iTfHOna5f39ConGgwIkVDVsDjfYqAW1
VPuwV1ExOWLjzIOtiiN2Xx62kqefgCRhVpc+qwIBIwKCAQBy6RTuV4FCw0tCAOBi
pFqtQsnGYqKO+UKsV0hAfDmA0u1wWRRXFV88WRhOyg5CdfWC+VnEHXh0KYmVEmoU
4XwgB9yrUJAol4t5/0SR1kSXKD60ivC6fQbh1r0tYqYBAgV+IO5Vr8qoeyMNX8Q5
ihQo4CuDwLsPLrQk1CMDdeQwFmTvcSeJ/KqEluVxoBqegKtWT52C4JIenp95I96Z
CaFhHWaY8XjSKSO07In8RoIp2v24DXtNHy4rd5vhgUi0HjAihEA93eRog4rDsHSB
1fm2rJVtuImDPnFMjH75d3SwYPyca+4ZLZwnXgMjE7PJFtUe0niEr40wsPuq4i5L
B6LrAoGBAPl/PnwPBdst4AhbNn8FmxLje/DZWtpmZoyITBDq129KCM4xGjS3FyDY
7l69VdaiiFDBXHVDQ6SxQ85z69rk45oGgaU0AVzOb+ZCfTocYb6/xcOVFhLc8h6E
HzdlW/vjyvYij+o5hNAyo+2VV7y8DZ92V0fMaVsxQzcU+6vKy6VRAoGBAPK/Jnqg
I0MWhP7zgWo4g+9TM67OxeYkXHV1UUEirjH7LQrMhomlJ7yEYUencfY1md/Fssl1
L1xRPXpiUSzmCRsAz5pn1pnSFRfdmj1uN8PlDBDYa/w9gIJ/Z1DtPdpG0mH4Hx0j
3LzEkVtMxHiusHVq7a7q8ZMMNEQpdSkPcJU7AoGBAIdw9gjU9IztBJbSbgpwweWu
sP8W6C1qyfSEgRB/fEO6ec8EtnRjZFOo9m3xwOI6+Yrsn+fir7EtB41U3x8Oii8K
2Koji7YJqnWvEMfGQ7CxP3jNRn9EvfNPCaG6rkbpX4zuMN48e0xzQwvx/G3FK/d6
waqiKpCXFdwStIHUfS3bAoGAUzo5FBmlsJoBtn9fkiIBWV5a3Nkt6IF+yS+JkqzO
AoIA0ICjJ+DabIUoqtpS9VQ0wcAgCo6T5SMrBWOJi7yVaFgMqfe3Sq5tochSI7DC
qZBb6IS3TysHfTL+2erwopvwXBqOUyI9DYU5Jp36OAFhElCMAXUfoCFxAW1MvZ7k
```

```
xXMCgYEApZ/k+CDP9R2gzq1vMAyG57Rq+/WDD748eb7bamesEvQuaZWpc/m+u7nV
pEQfHIxgOckaRkYnCHivOMRf8LUkNCoQ/hJoa3XV5hcb/jmXzcWpqSiB5eXqG/fv
AAWruTdhzpUo4dniY/ZYvAaIbgk7R8hjKc2t07u58on8E7DlhZ4=
-----END RSA PRIVATE KEY-----
```

将上文阴影内容复制粘贴进新建的文本文档中，并将其更名为“RSA-201801-openssh”，将该 txt 文件保存在本地供使用。

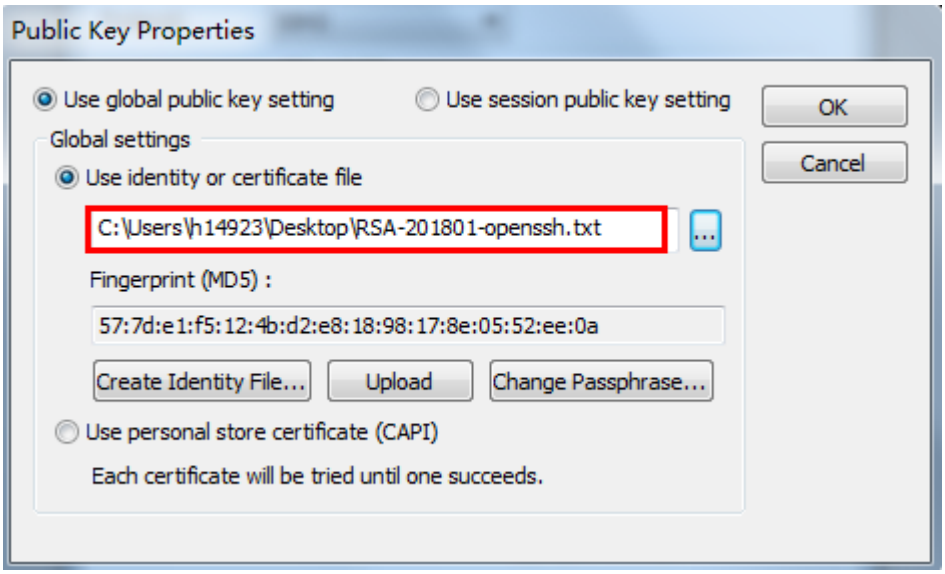
(1) 打开 secureCRT 工具（版本至少 6.5 以上），点击快速连接，在主机名一栏中填入运维审计系统的 IP 地址。用户名栏输入“root”，并将公钥认证移至首行。

图2 新建连接



(2) 选择“公钥”后点击右边的属性，在公钥属性窗口中指定密钥（RSA-201801-openssh.txt）的存放路径。

图3 指定密钥路径



(3) 登录后即可进入 Main menu 菜单。

图4 Main menu 菜单

```
Main Menu
    1. Date and Time
    2. Network Configuration
    3. Service Management
    4. Administrators
    H. High Availability
    S. System Status
    T. System Tools
    R. System Recovery
    A. Application Server
Enter selection:
```

4.5.2 分别配置主备机IP地址

登录 Main menu 菜单。

按照索引选择“2”，进入“Network Configuration”。

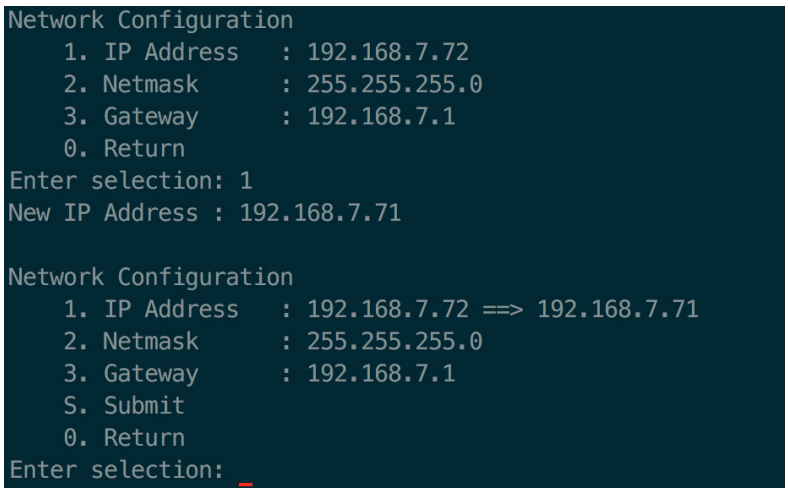
选择对应数据网口前的索引，进行网络配置。

网络接口与 HA 接口都需要配置 IP 地址。

图5 网络配置菜单

选择相应的配置项编号即可修改该配置参数，例如：选择 1（IP Address），修改该网卡的 ip 地址，回车之后菜单中会提示您新设置的 IP 地址，确认没问题之后选择 S（submit）进行提交生效。

图6 修改 IP 地址



选择“S”提交配置更改。

4.5.3 分别配置主备机NTP(可选)

登录 Main menu 菜单。

按照索引选择“1”，进入“Date and Time”,再选择“3”，进入“Network Time Protocol”。

图7 NTP 设置

```
Main Menu
    1. Date and Time
    2. Network Configuration
    3. Service Management
    4. Administrators
    H. High Availability
    S. System Status
    T. System Tools
    R. System Recovery
    A. Application Server
Enter selection: 1

Date and Time
    1. Date : 2018-01-18
    2. Time : 15:07:52
    3. Network Time Protocol
    0. Return
Enter selection: 3
```

添加时钟服务器。

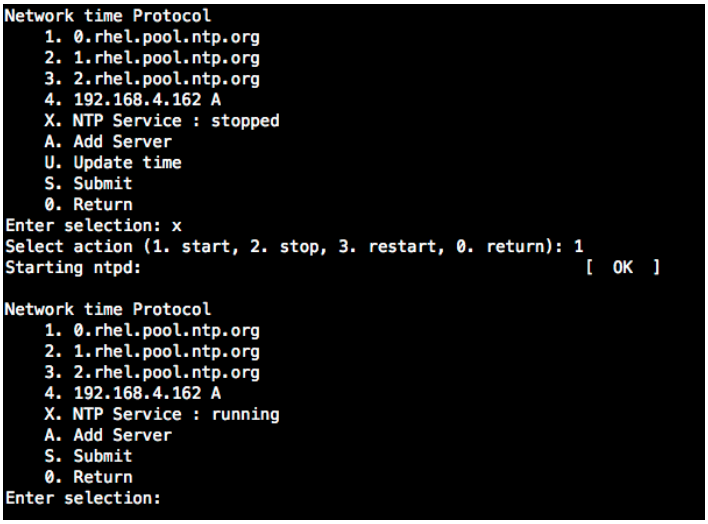
图8 添加时钟服务器

```
Network time Protocol
    1. 0.rhel.pool.ntp.org
    2. 1.rhel.pool.ntp.org
    3. 2.rhel.pool.ntp.org
    X. NTP Service : stopped
    A. Add Server
    U. Update time
    0. Return
Enter selection: a
Please input new NTP server :192.168.4.162

Network time Protocol
    1. 0.rhel.pool.ntp.org
    2. 1.rhel.pool.ntp.org
    3. 2.rhel.pool.ntp.org
    4. 192.168.4.162 A
    X. NTP Service : stopped
    A. Add Server
    U. Update time
    S. Submit
    0. Return
Enter selection:
```

启动 NTP Service 服务

图9 启动服务



提示

NTP 不是配置 HA 必要选项，但时钟不同步会导致 HA 节点状态异常。

4.5.4 配置主机HA

使用超级管理员登录主机运维审计系统。

进入[系统设置/HA 安装]页面，在双机部署中选择[主机配置]。

在[主机信息]中，为网络接口与 HA 接口选择网卡接口。

在[备机信息]中，填写网络接口与 HA 接口的 IP 地址。

在[常规配置]，填写“浮动 IP”与“Ping IP”。

点击<执行安装>按钮。

图10 HA 主机配置示意图

图11 主机部署成功

4.5.5 配置备机HA

当主机虚 IP 可以访问后，使用超级管理员登录备机运维审计系统。

进入[系统设置/HA 安装]页面。

选择双机部署为“[备机配置]”。

填写主机网络接口 IP 地址。

点击<执行安装>按钮。

图12 HA 备机配置示意图

图13 备机部署成功

4.6 验证配置

4.6.1 使用虚IP登录运维审计系统。

(1) 使用虚 IP 可以登录运维审计系统。

(2) 打开右上角向下箭头中的[HA 状态]页面，可查看 HA 状态。

(3) 点击<执行数据同步>，测试数据是否可正常同步。

图14 HA 状态示意图

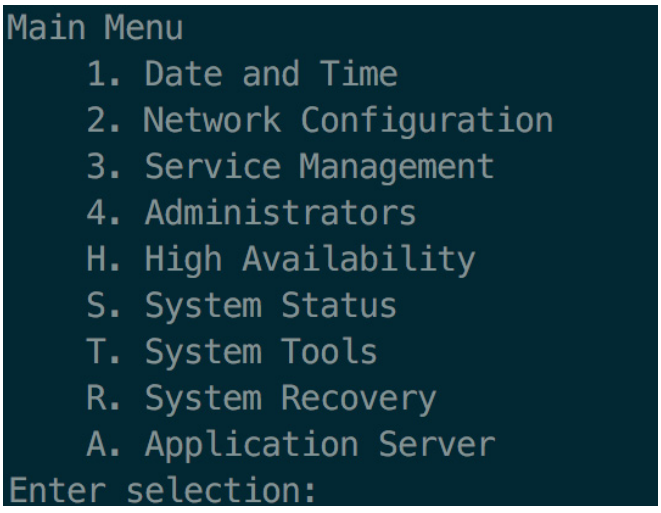
提示

首次登陆时，可能会提示“备机同步数据失败”，手动执行数据同步即可。

4.6.2 登录Main menu查看HA状态

(1) 登陆主机的 Main menu 菜单。

图15 Main menu 菜单



(2) 选择 H 进入 High Availability。

图16 High Availability 菜单

```
High Availability Configuration
    1. Normal Sync(do at standby)
    T. Takeover
    S. Standby
    X. Status
    0. Return
Enter selection:
```

(3) 选择 X，查看当前节点 HA 运行状态。

图17 HA 状态

```
High Availability Configuration
    1. Normal Sync(do at standby)
    T. Takeover
    S. Standby
    X. Status
    0. Return
Enter selection: x
hbstatus, rscstatus | node2: nodestatus, GE0_0, GE0_1 | node1: nodestatus, GE0_0, GE0_1 | 192.168.7.1: nodestatus, 192.168.7.1 |
-------------------------------------------------------------------------------------------------------------------------------

running, all | active, up | , up | active, up | , up | ping, up |
running, all | active, up | , up | active, up | , up | ping, up |
running, all | active, up | , up | active, up | , up | ping, up |
running, all | active, up | , up | active, up | , up | ping, up |
running, all | active, up | , up | active, up | , up | ping, up |
```

说明

“running”表示 ha 服务正在运行。“all”表示当前节点为主机。“none”表示当前节点为备机。

4.6.3 HA切换测试

(1) 登陆 Main menu 菜单，选择 H 进入 High Availability 选项。

图18 High Availability 菜单

```
High Availability Configuration
    1. Normal Sync(do at standby)
    T. Takeover
    S. Standby
    X. Status
    0. Return
Enter selection:
```

(2) 查看当前节点状态，如果当前节点为“all”，则选择“S”选项，使当前节点变为备节点。

图19 切换 HA

```
High Availability Configuration
    1. Normal Sync(do at standby)
    T. Takeover
    S. Standby
    X. Status
    0. Return
Enter selection: s
Are you sure?(y/n) y
Going standby [all].
```

(3) 切换成功后，节点状态由“all”为“none”。

图20 主节点切换为备节点

```
High Availability Configuration
    1. Normal Sync(do at standby)
    T. Takeover
    S. Standby
    X. Status
    0. Return
Enter selection: x
hbstatus, rscstatus | node2: nodestatus, GE0_0, GE0_1 | node1: nodestatus, GE0_0, GE0_1 | 192.168.7.1: nodestatus, 192.168.7.1 |
-------------------------------------------------------------------------------------------------------------------------------
running, transition | active, up | , up | active, up | , up | ping, up |
running, transition | active, up | , up | active, up | , up | ping, up |
running, transition | active, up | , up | active, up | , up | ping, up |
running, none | active, up | , up | active, up | , up | ping, up |
running, none | active, up | , up | active, up | , up | ping, up |
```

说明

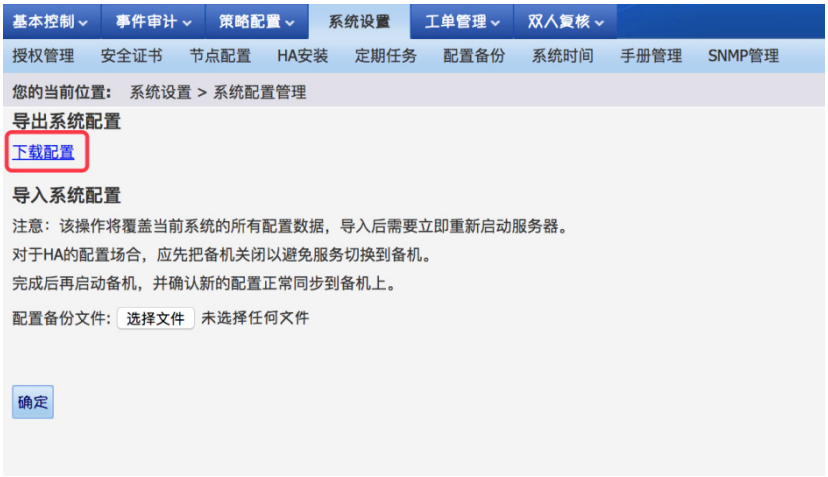
操作前，应确定当前节点状态。在主机节点应选择 S 选项切换为备节点。在备机节点应选择 T 选项，切换为主机节点。

4.6.4 HA配置备份

(1) 使用超级管理员登录运维审计系统。

(2) 打开[系统设置/配置备份]，在导出系统配置中点击<下载配置>。

图21 配置备份



(3) 保存导出的配置备份文件即可。

4.6.5 HA拆除

1. 主节点退出HA

(1) 使用超级管理员登录虚 IP，打开[系统设置/HA 安装]。

(2) 点击<退出 HA>按钮，并在弹出的提示框确认操作。

(3) 节点退出 HA 后，需要重新启动系统。

图22 退出 HA

2. 备节点退出HA

(1) 使用超级管理员登录虚 IP，打开[系统设置/HA 安装]。

(2) 点击<退出 HA>按钮，并在弹出的提示框确认操作。

(3) 节点退出 HA 后，需要重新启动系统。

图23 备节点退出 HA

说明

由于主节点退出 HA 后，再登录运维审计系统时会提示：“HA 状态错误：备机数据同步失败，备点失败...”属正常现象。

Radius 认证配置举例

目 录

1 简介

RADIUS 是一种用于在需要认证其链接的网络访问服务器（NAS）和共享认证服务器之间进行认证、授权和记帐信息的文档协议。

RADIUS 在运维审计系统中，主要体现的是认证功能。

2 配置前提

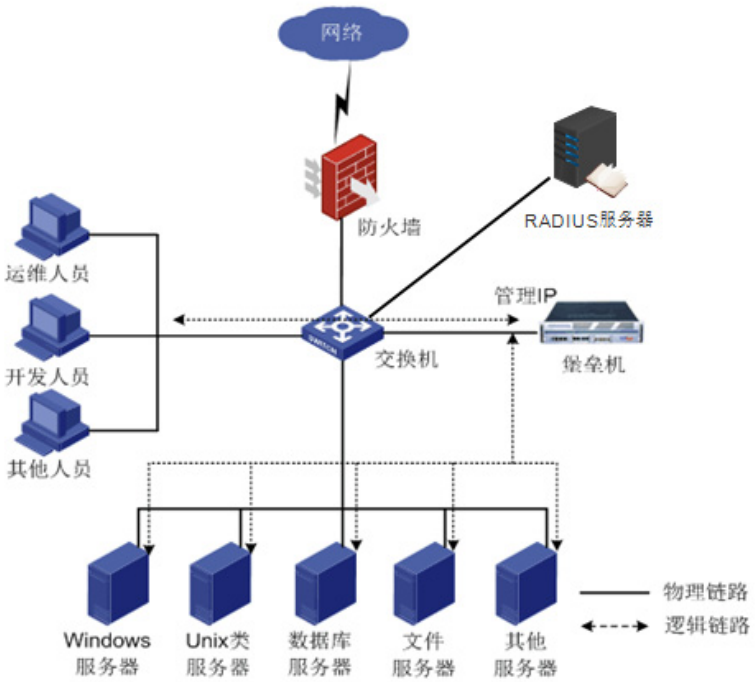
收集 RADIUS 服务器信息：IP 地址、RADIUS 端口号、RADIUS 的通信密码。

- 典型 Radius 服务器配置
  - 状态：启用服务器 1
  - 名称：radius
  - RADIUS 服务器 1：192.168.6.220，端口：1812，通讯密码：123456
  - RADIUS 服务器 2：192.168.6.221，端口：1812，通讯密码：123456

3 配置举例

3.1 组网需求

图1 RADIUS 认证网络图



3.2 系统版本要求

适用产品版本：ESS 6102

3.3 创建RADIUS认证方式

登录“超级管理员”，“策略配置 > 身份验证”，选择“radius”，点击“新建”。

图2 创建 RADIUS 认证方式

配置 RADIUS 认证方式：

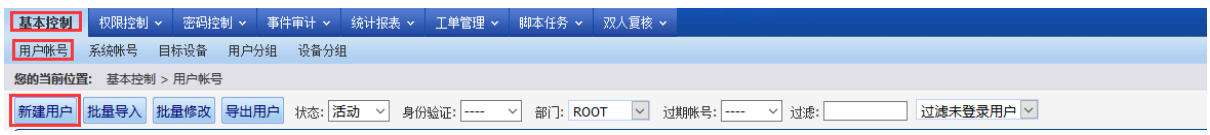
- 状态：选择为启用服务器 1。
- 名称：该 radius 认证的名称。
- RADIUS 服务器 1：IP 地址：填写 RADIUS 的 IP 地址。
- 端口：填写 RADIUS 的认证端口，一般默认为 1812。
- 通信密码：填写 RADIUS 的通信密码。

图3 配置 RADIUS 认证方式

3.4 创建用户，绑定RADIUS认证方式

“基本控制 > 用户账号”，点击“新建用户”。

图4 创建用户



- 登录名：登录运维审计系统的账户名。
- 真实姓名：该账户名的真实用户。
- 部门：选择相应的部门。
- 身份验证方式：这里选择之前配置的 radius。

- radius 用户名：绑定该登录名对应的 radius 账户，如果不填，则默认此项为登录名。

图5 配置用户信息

3.5 登录认证

图6 用户登录

3.6 验证配置

(1) 进入超级管理员账户，选择“策略配置 > 身份验证”，选择相应的 radius 认证，点击“测试”。

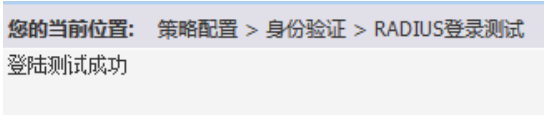
图7 身份验证

(2) 填写需要验证的账户密码，选择相应的服务器，点击“确定”。

图8 配置账户密码

(3) 返回“登录测试成功”。

图9 登录成功



TOTP 令牌（动态令牌）配置举例

目 录

1 简介

TOTP 是基于时间的一次性密码算法的简称。这个算法通过一个共享密钥和当前时间来计算一次性密码。经常被用于双因素认证的系统中。因为网络延时或者时钟没有完全同步的原因，一般生成一次密码，需要 60 秒的发送间隔。

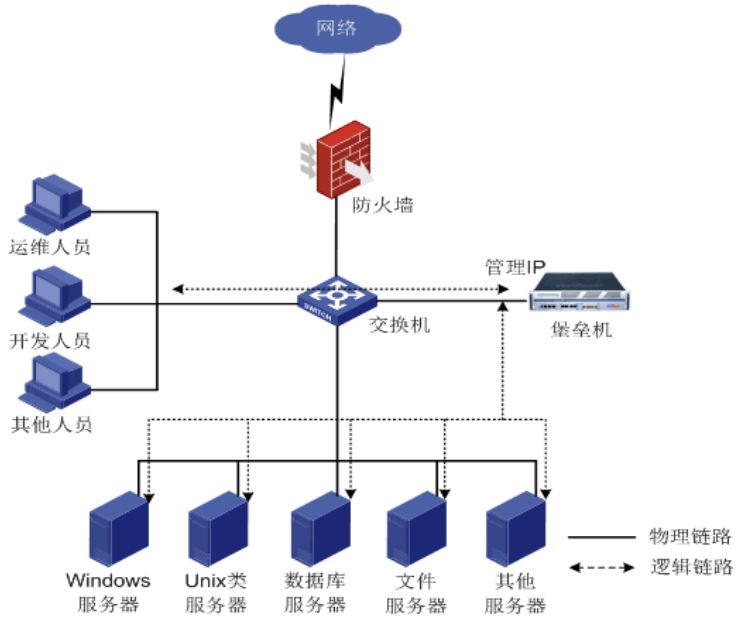
2 配置前提

因为 TOTP 令牌与时间密切相关，所以在配置 TOTP 令牌前，请确保运维审计系统的时间与北京时间一致。

3 配置举例

3.1 组网需求

图1 TOTP 令牌认证网络图



3.2 系统版本要求

适用产品版本：ESS 6102。

3.3 新建TOTP认证方式

(1) 超级管理员，“策略配置 > 身份验证”，选择“totp”，点击“新建”。

图2 新建 TOTP 认证方式

(2) 修改属性

- 状态：选择为启用。
- 名称：填写此 totp 名称。

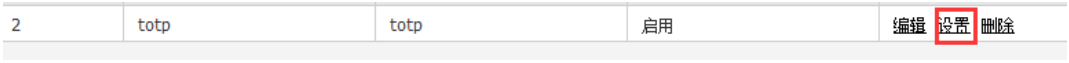
点击确定。

图3 修改属性

3.4 TOTP令牌管理

点击“设置”。

图4 TOTP 令牌管理



3.4.1 单个令牌管理

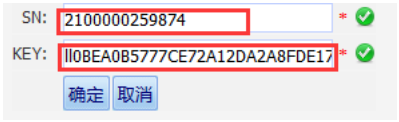
1. 导入令牌

(1) 点击“新建”。

图5 导入令牌

(2) 输入对应的 key 和 SN 号码，点击“确定”。

图6 输入对应的 key 和 SN 号码



2. 令牌同步

方法一：

(1)　当令牌使用一段时间之后，可能由于时钟漂移，导致一次性密码产生错误，这时需要同步令牌。选择相应令牌，点击“同步”。

图7 同步令牌

(2)　将令牌产生的两个一次性密码，依次填入“密码 1”、“密码 2”。点击“同步”。

图8 输入密码

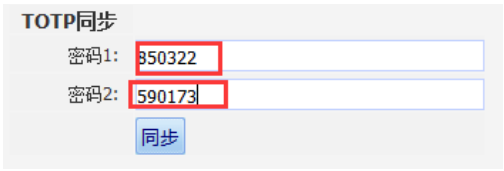
方法二：

(1)　页面右上角，进入“账户设置”

图9 账户设置

(2)　将令牌产生的两个一次性密码，依次填入“密码 1”、“密码 2”。点击“同步”。

图10 输入密码

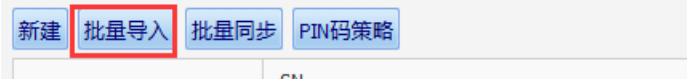


3.4.2 批量令牌管理

1. 批量导入令牌

(1) 点击“批量导入”。

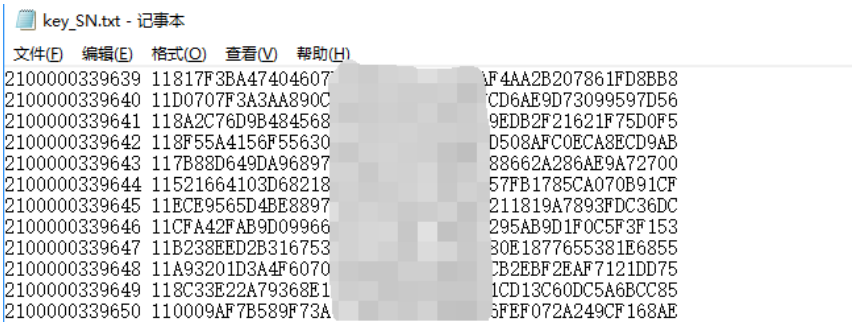
图11 批量导入令牌



(2) 将 key 和 SN 号写入文本。

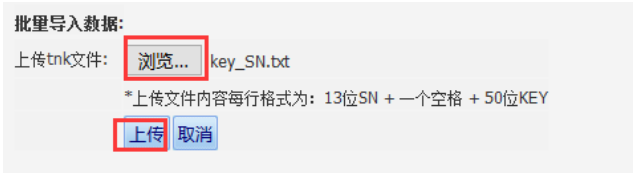
格式：13 位 SN + 一个空格 + 50 位 KEY。

图12 将 key 和 SN 号写入文本



(3) 导入该文本。

图13 导入文本



(4) 点击“确定导入”。

图14 确认

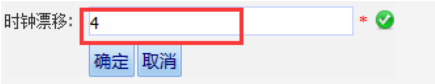
2. 批量同步令牌

(1) 点击“批量同步”。

图15 批量同步令牌

(2) 设置时钟漂移，然后点击确定。

图16 设置时钟漂移



3.4.3 PIN码策略

TOTP 令牌不能单独作为验证工具，必须与另外的静态密码进行绑定，我们在运维审计系统中，将这个静态密码称为 PIN 码。

点击“PIN 码策略”。

图17 PIN 码策略

设置需要的 PIN 码复杂度。

图18 设置 PIN 码复杂度

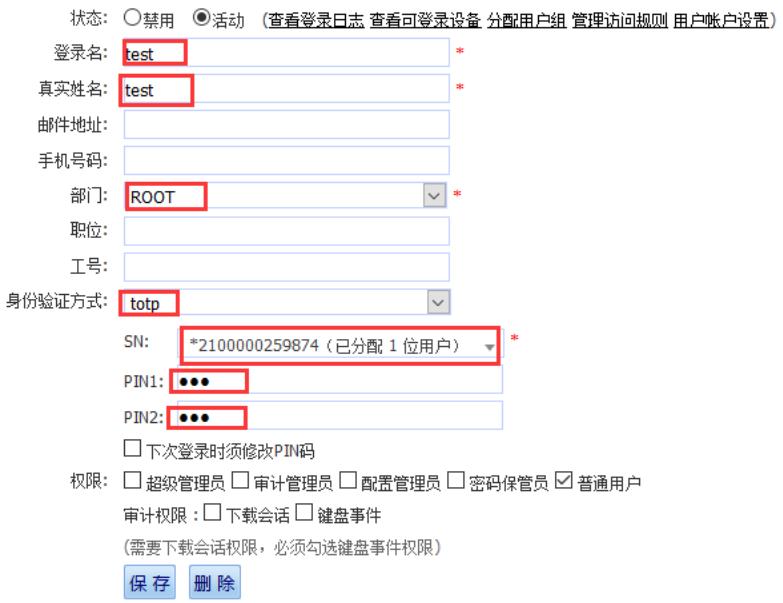
3.5 创建用户，绑定TOTP令牌

“基本控制 > 用户账号 > 新建用户”。

图19 创建用户

- 登录名：登录运维审计系统的账户名。
- 真实姓名：该账户名的真实用户。
- 部门：选择相应的部门。
- 身份验证方式：这里选择之前配置的 totp。
- SN：选择需要绑定的令牌 SN（一个令牌最多可以分配给 5 个用户使用）。
- PIN1：用户登录时使用的静态密码。
- PIN2：用户做双人授权时使用的静态密码。

图20 配置用户信息



3.6 TOTP使用

3.6.1 TOTP登录

输入账户、密码。

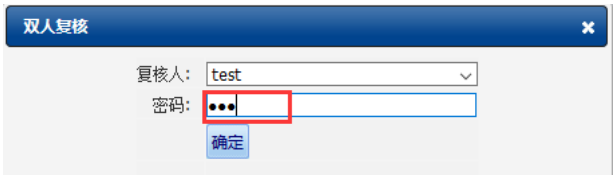
密码格式为：PIN1 码+令牌

图21 TOTP 登录

3.6.2 TOTP双人复核

密码：输入 PIN2 码。

图22 TOTP 双人复核



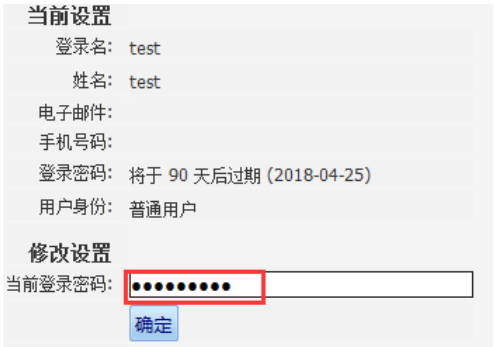
3.6.3 TOTP修改PIN1、PIN2 码

(1) 页面右上角，进入“账户设置”

图23 账户设置

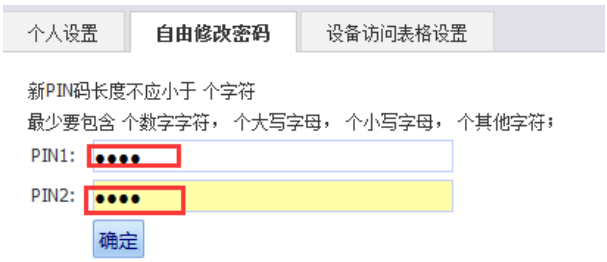
(2) 输入：PIN1 码+令牌

图24 PIN1 码+令牌



(3) 切换到“自由修改密码”，修改 PIN1、PIN2 码。

图25 修改 PIN1、PIN2 码



不托管密码模式配置举例

目 录

1 简介

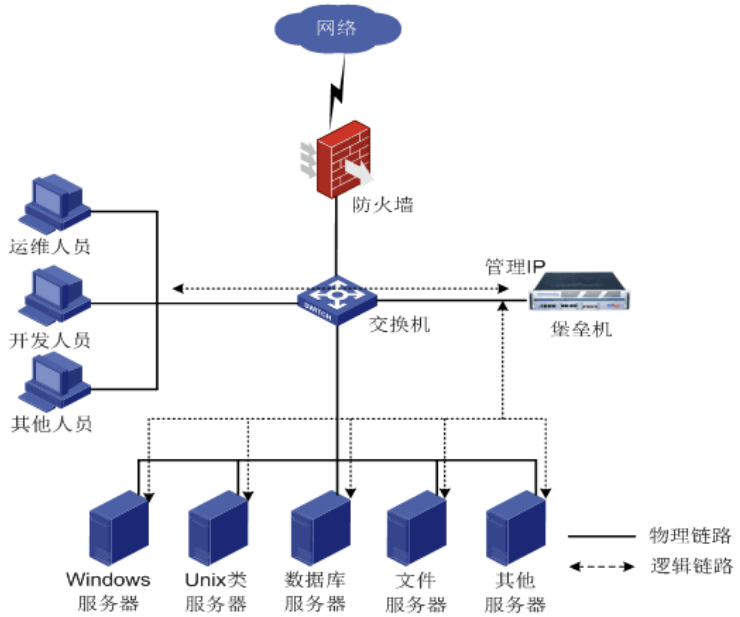
不托管密码模式是指运维审计系统不托管目标设备的密码。普通用户通过运维审计系统登录目标设备，需要手工输入密码。

运维审计系统中的“any”系统账号，用于未托管密码的场景，代表任意账号。

2 配置举例

2.1 组网需求

图1 运维审计系统网络图



2.2 系统版本要求

适用产品版本：ESS 6102。

2.3 配置思路

(1) 新建目标设备，不托管密码。

(2) 在访问规则中关联 any 账号。

(3) 普通用户访问是自行输入账号和密码。

2.4 配置步骤

2.4.1 关联相应设备any账户的访问规则

登录“配置管理员”，“权限控制 > 访问权限”。

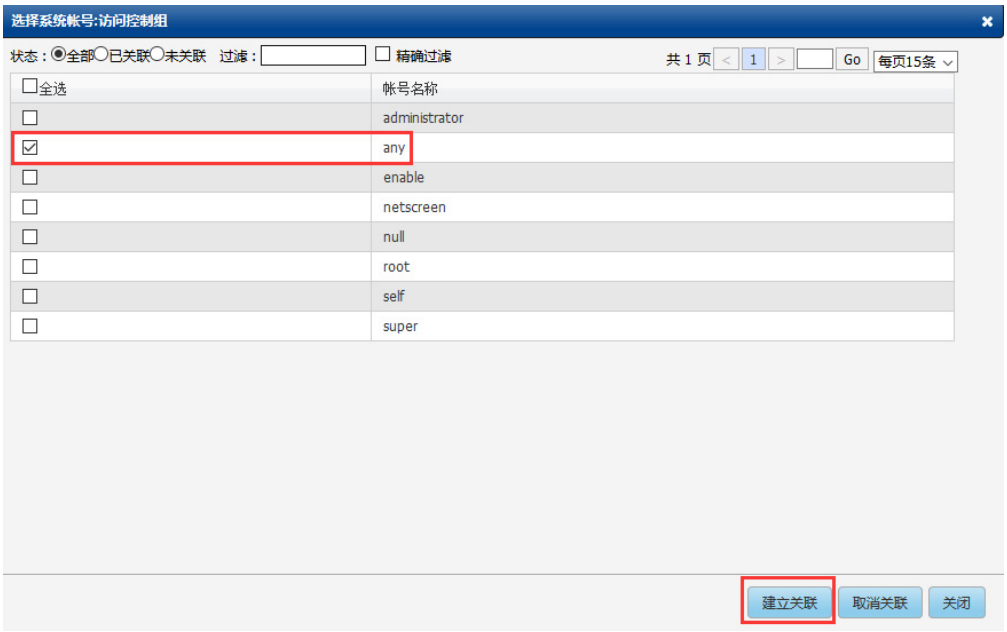
图2 配置访问权限

选择对应的规则，点击“系统账号”。

图3 选择规则

选择“any”账户，点击“建立关联”。

图4 建立关联



2.4.2 登录设备

选择相应账户登录，切换到普通用户。

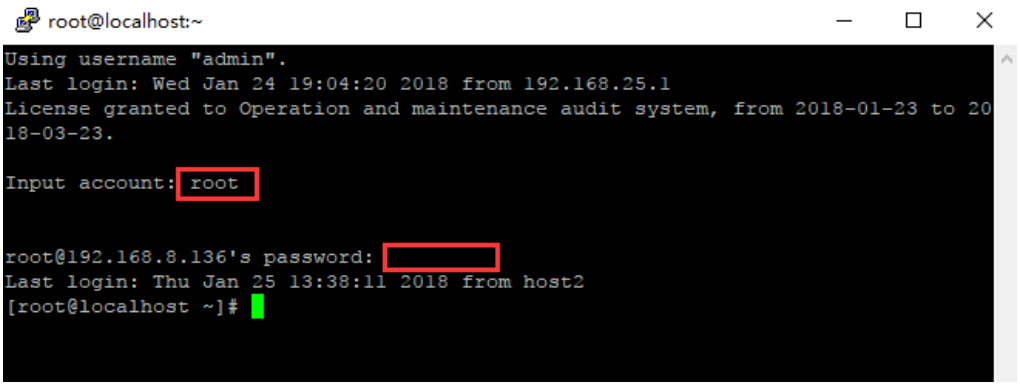
选择相应的目标设备，右键点击相应服务，选择“any”账户。点击确定。

图5 登录设备

字符类型设备：

手工输入账户、密码。

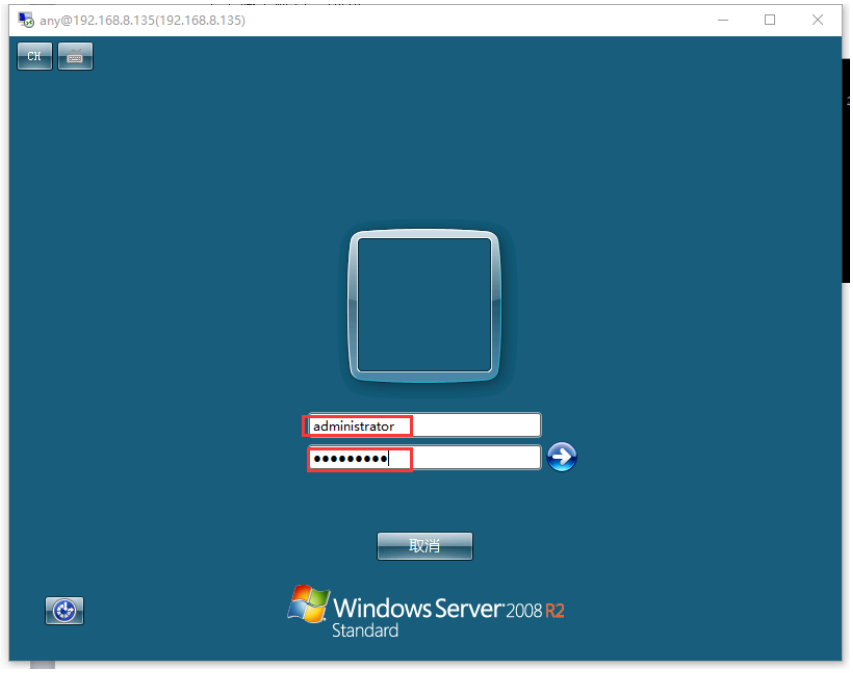
图6 字符类型设备



图形类型设备：

手工输入账户、密码。

图7 图形类型设备


any@192.168.8.135(192.168.8.135)
Ctrl
administrator
取消
Windows Server 2008 R2
Standard

部门分权配置举例

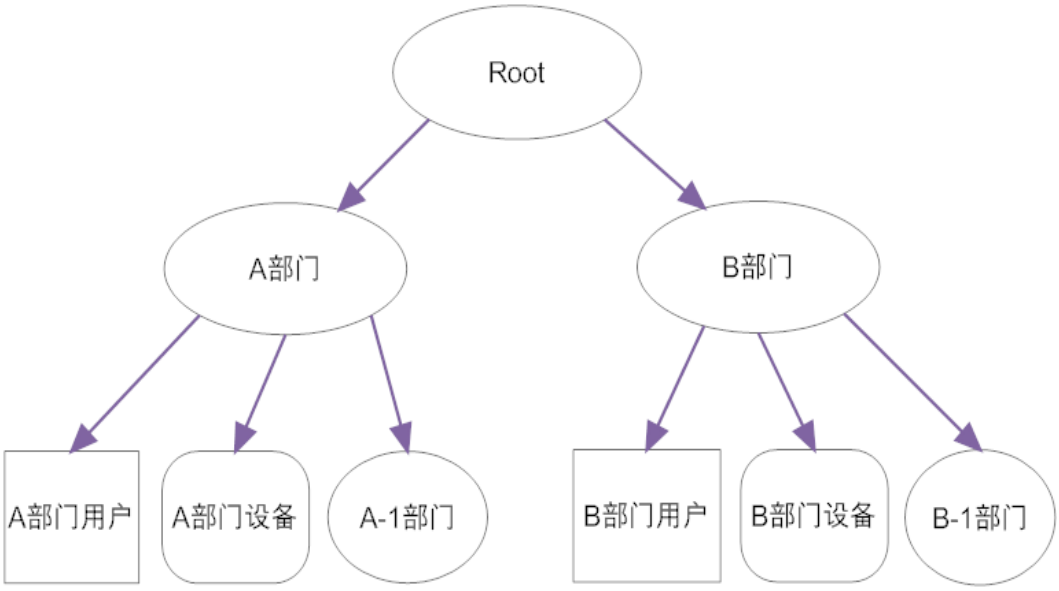
目 录

1 简介

本文档介绍如何对运维审计系统配置部门分权。

运维审计系统中可以对用户账号、目标设备以及访问权限进行部门划分，方便用户按照部门来管理用户和设备。运维审计系统中部门的结构类似于树形结构，最顶层的部门是 ROOT，往下可以由用户自定义部门结构。

图1 部门分权组网图



2 配置前提

本文档不严格与具体软、硬件版本对应，如果使用过程中与产品实际情况有差异，请以设备实际情况为准。

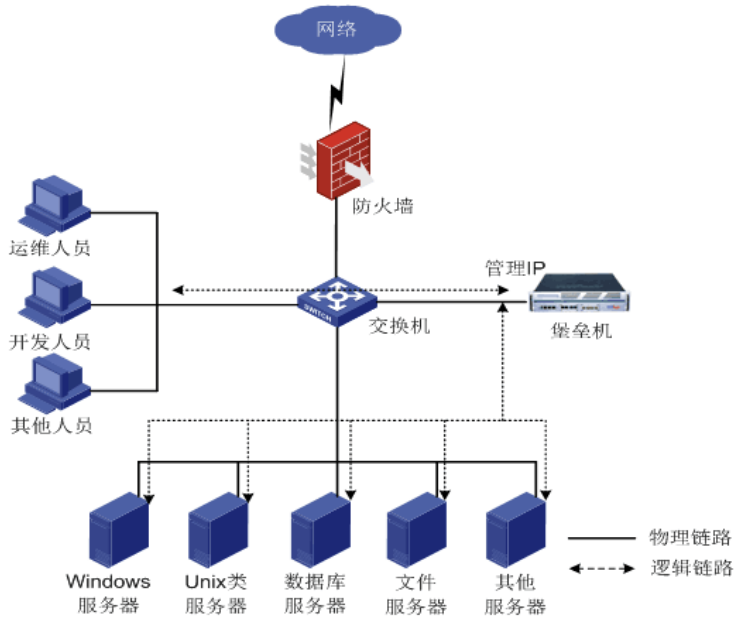
本文档中的配置均是在实验室环境下进行的配置和验证，配置前设备的所有参数均采用出厂时的缺省配置。如果您已经对设备进行了配置，为了保证配置效果，请确认现有配置和以下举例中的配置不冲突。

本文档假设您已了解部门分权所带来的特性。

3 配置举例

3.1 组网需求

图2 运维审计系统组网图



3.2 系统版本要求

适用产品版本：ESS 6102。

3.3 配置思路

- 建立部门。
- 为用户账号和目标设备分配部门。

3.4 配置步骤

3.4.1 新建部门

(1) 使用超级管理员身份登录运维审计系统，选择[策略配置/部门配置]。

图3 部门分权配置图

(2) 在[部门配置]页面中，单击相应部门名称栏目右侧动作列中<新建>按钮。

(3) 在跳转的[新建]部门页面中，输入新建部门名称，选择该部门隶属部门，单击<确定>按钮，完成部门新增。

图4 新建部门名称

说明

第一次新建部门时，只能隶属于初始的 ROOT 部门。

3.4.2 部门编辑

(1) 使用超级管理员身份登录运维审计系统，选择[策略配置/部门配置]。

(2) 在[部门配置]页面中，在需要更换隶属部门的部门名称栏目右侧动作列中单击<编辑>按钮。

(3) 在跳转的[编辑]页面中，从隶属于下拉菜单中选择需要更换到的部门名称，单击<确定>按钮。

3.4.3 部门删除

(1) 使用超级管理员身份登录运维审计系统，选择[策略配置/部门配置]。

(2) 在[部门配置]页面中，在需要删除或撤销部门名称栏目右侧动作列中单击<编辑>按钮。

(3) 在跳转的[编辑]页面中，单击<删除>按钮即可删除不需要的部门。

3.4.4 分配设备所属部门

(1) 使用隶属于 ROOT 部门的配置管理员登录运维审计系统，选择[基本控制/目标设备]。

(2) 在[目标设备]页面中，单击需要调整设备栏目右侧<编辑>按钮。

图5 设备配置页面

(3) 在弹出的[设备编辑]页面中，在部门下拉菜单中选择目标设备分配到指定的部门，单击<确定>按钮。

图6 设备所属部门配置

3.4.5 分配用户所属部门

(1) 使用超级/配置管理员身份登录运维审计系统，选择[基本控制/用户账号]。

图7 用户配置页面

(2) 在[用户帐号]页面中，单击<新建用户>按钮或在已有的帐号栏目右侧点击<管理>按钮，在新页面中，输入相关用户信息，在部门下拉菜单中选择该用户分配到的部门即可。

图8 用户所属部门配置

单击<保存>按钮，完成部门管理员/普通用户的部门分配。

说明

无法修改缺省管理员部门属性。

3.4.6 分配访问权限所属部门

使用配置管理员身份登录运维审计系统，选择[权限控制/访问权限]。

单击<新建>按钮或在已有的访问权限条目右侧点击<编辑>按钮，弹出的新窗口后，在部门下拉菜单中选择需要修改的部门即可。

图9 访问权限

3.4.7 分配改密计划所属部门

(1) 使用配置管理员身份登录运维审计系统，选择[密码控制/改密计划]。

(2) 单击<新建计划>按钮或在已有的改密计划条目右侧点击<编辑>按钮，跳转到新窗口后，在部门下拉菜单中选择需要修改的部门即可。

3.4.8 部门分权模式下的命令权限管理

命令权限为全局设置，只有 Root 部门的配置管理员可以进行配置和修改。

3.5 配置验证

1. 查看用户

确认管理员只能查看本部门及下级部门用户。

(1) 使用系统运维组配置管理员登录运维审计系统，选择[基本控制/用户账号]。

图10 用户列表

(2) 使用部门选项进行过滤，只能选择当前部门与下级部门。

图11 部门过滤

2. 查看设备

确认管理员只能查看本部门及下级部门的设备。

(1) 使用系统运维组配置管理员登录运维审计系统，选择[基本控制/目标设备]。

图12 设备列表

(2) 使用部门选项进行过滤，只能选择当前部门与下级部门。

图13 部门过滤

3. 查看访问权限

确认管理员只能查看本部门及下级部门的访问权限。

(1) 使用系统运维组配置管理员登录运维审计系统，选择[基本控制/目标设备]。

图14 访问权限列表

(2) 使用部门选项进行过滤，只能选择当前部门与下级部门。

图15 部门过滤

4. 查看改密计划

确认管理员只能查看本部门及下级部门的访问权限。

使用系统运维组配置管理员登录运维审计系统，选择[密码控制/改密计划]。

图16 改密计划列表

单机配置举例

目 录

1 简介

本文档介绍如何部署单台运维审计系统。

2 配置前提

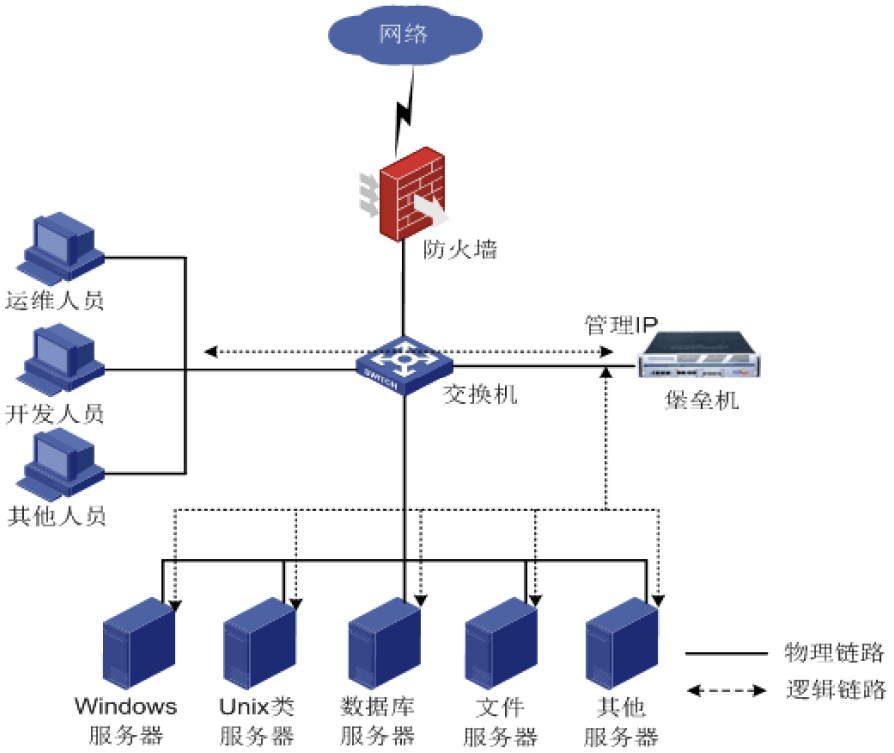
需要满足如下条件：

- 分配 1 个 IP 地址，用于用户登录访问。
- 配置 NTP 服务器，保证时间同步。
- 运维审计系统与被管理设备之间路由可达、协议可通。
- PC 端只可访问运维审计系统的 22、443、3389 与 5899 端口。

2.1 组网需求

运维审计系统以物理旁路，逻辑串联的方式部署在核心网络中。作为运维审计的唯一入口。

图1 单机部署组网图



2.2 系统版本要求

适用产品版本：ESS 6102。

2.3 配置步骤

1. 登录Main menu菜单

通过连接键盘、显示器到物理机登录 Main menu 菜单，用户名密码为 root/admin。

通过 SSH 远程连接登录 Main menu 菜单，使用密钥进行加密认证。

提示

密钥为登陆运维审计系统后台管理菜单的唯一认证方式。

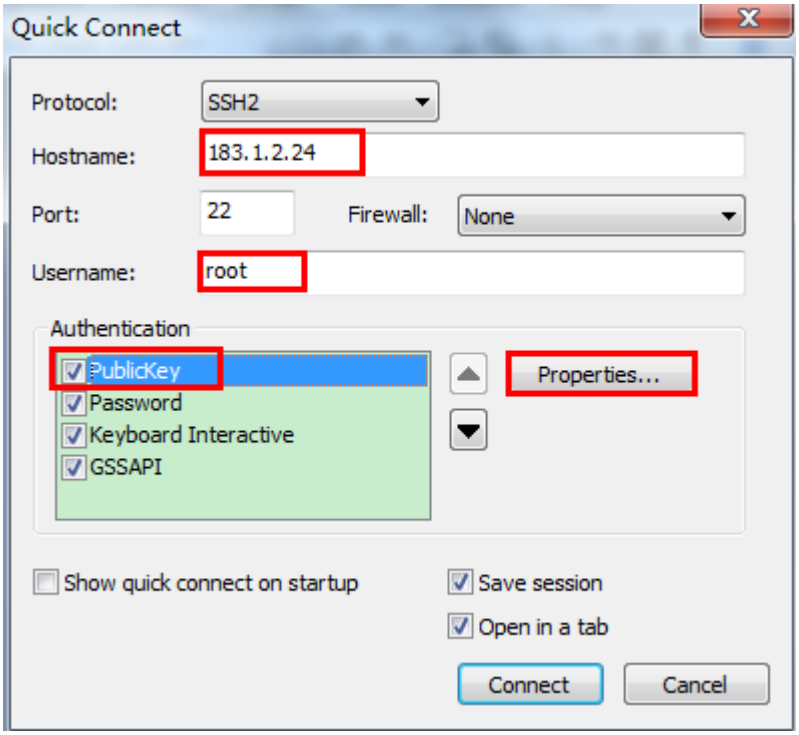
运维审计系统的密钥内容如下：

```
-----BEGIN RSA PRIVATE KEY-----
MIIEogIBAAKCAQEA7JSUgUq+1L9AlvK+6TRCN4mBTSVszAEu6llYhMOFcqM0I4o4
74ZaqWwi/JDwLnpi4HnW7h6OlM39I9qeKv1o9qbGUaXdgL+IkcJB4PVgCgeQKGlZ
B3ng/iOFe47dTV6Dx3D5v3j7lxuihPJXwcHtRRjSD0GBH0IJeQAL2fK3rk4ldqhI
FouqgoyjdONrV0YInRdNWzpl2Nxob33B/U4pwdvKVqDzWDk17+tZEdFvaoqzXFgt
hGfnmDtNiGVSLrJjbH+lwN0JHVeUSZHQ0iTfHOna5f39ConGgwIkVDVsDjfYqAW1
VPuwV1ExOWLjzIOtiiN2Xx62kqefgCRhVpc+qwIBIwKCAQBy6RTuV4FCw0tCAOBi
pFqtQsnGYqKO+UKsV0hAfDmA0u1wWRRXFV88WRhOyg5CdfWC+VnEHXh0KYmVEmoU
4XwgB9yrUJAol4t5/0SR1kSXKD60ivC6fQbh1r0tYqYBAgV+IO5Vr8qoeyMNX8Q5
ihQo4CuDwLsPLrQk1CMDdeQwFmTvcSeJ/KqEluVxoBqegKtWT52C4JIenp95I96Z
CaFhHWaY8XjSKSO07In8RoIp2v24DXtNHy4rd5vhgUi0HjAihEA93eRog4rDsHSB
1fm2rJVtuImDPnFMjH75d3SwYPyca+4ZLZwnXgMjE7PJFtUe0niEr40wsPuq4i5L
B6LrAoGBAPl/PnwPBdst4AhbNn8FmxLje/DZWtpmZoyITBDq129KCM4xGjS3FyDY
7l69VdaiiFDBXHVDQ6SxQ85z69rk45oGgaU0AVzOb+ZCfTocYb6/xcOVFhLc8h6E
HzdlW/vjyvYij+o5hNAyo+2VV7y8DZ92V0fMaVsxQzcU+6vKy6VRAoGBAPK/Jnqg
I0MWhP7zgWo4g+9TM67OxeYkXHV1UUEirjH7LQrMhomlJ7yEYUencfY1md/Fssl1
L1xRPXpiUSzmCRsAz5pn1pnSFRfdmj1uN8PlDBDYa/w9gIJ/Z1DtPdpG0mH4Hx0j
3LzEkVtMxHiusHVq7a7q8ZMMNEQpdSkPcJU7AoGBAIdw9gjU9IztBJbSbgpwweWu
sP8W6C1qyfSEgRB/fEO6ec8EtnRjZFOo9m3xwOI6+Yrsn+fir7EtB41U3x8Oii8K
2Koji7YJqnWvEMfGQ7CxP3jNRn9EvfNPCaG6rkbpX4zuMN48e0xzQwvx/G3FK/d6
waqiKpCXFdwStIHUfS3bAoGAUzo5FBmlsJoBtn9fkiIBWV5a3Nkt6IF+yS+JkqzO
AoIA0ICjJ+DabIUoqtpS9VQ0wcAgCo6T5SMrBWOJi7yVaFgMqfe3Sq5tochSI7DC
qZBb6IS3TysHfTL+2erwopvwXBqOUyI9DYU5Jp36OAFhElCMAXUfoCFxAW1MvZ7k
xXMCgYEApZ/k+CDP9R2gzq1vMAyG57Rq+/WDD748eb7bamesEvQuaZWpc/m+u7nV
pEQfHIxgOckaRkYnCHivOMRf8LUkNCoQ/hJoa3XV5hcb/jmXzcWpqSiB5eXqG/fv
AAWruTdhzpUo4dniY/ZYvAaIbgk7R8hjKc2t07u58on8E7DlhZ4=
-----END RSA PRIVATE KEY-----
```

将上文阴影内容复制粘贴进新建的文本文档中，并将其更名为“RSA-201801-openssh”，将该 txt 文件保存在本地供使用。

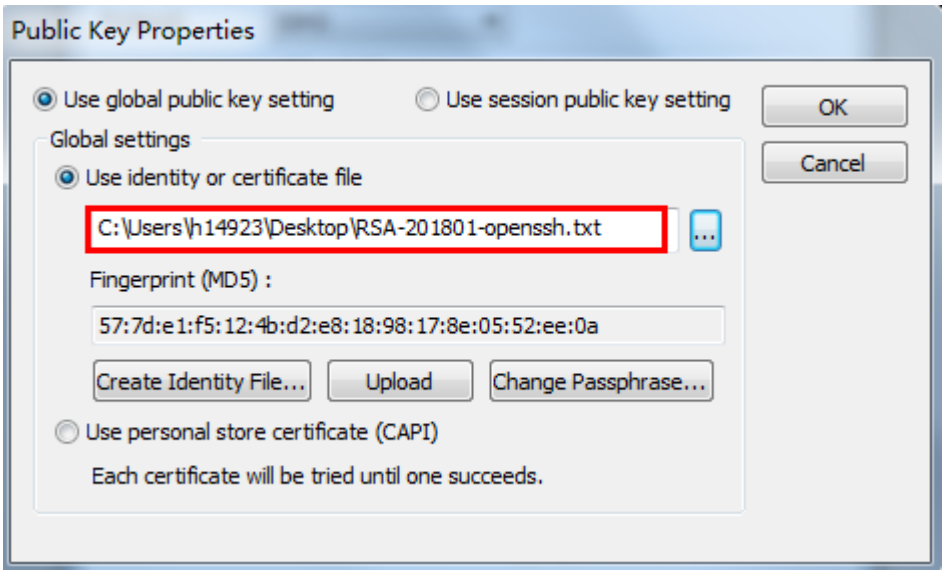
(1) 打开 secureCRT 工具（版本至少 6.5 以上），点击快速连接，在主机名一栏中填入运维审计系统的 IP 地址。用户名栏输入“root”，并将公钥认证移至首行。

图2 新建连接



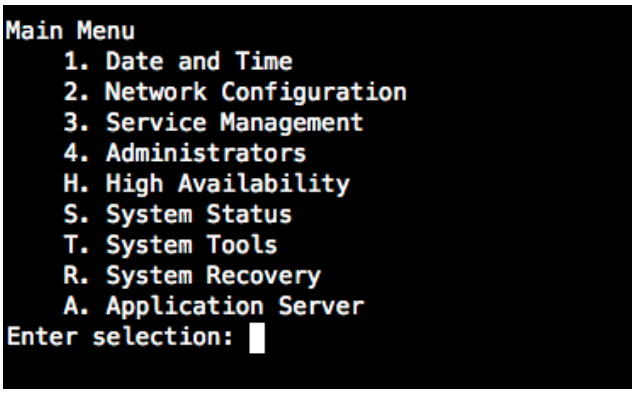
(2) 选择“公钥”后点击右边的属性，在公钥属性窗口中指定**密钥**（RSA-201801-openssh.txt）的存放路径。

图3 指定密钥路径



(3) 登录后即可进入 Main menu 菜单。

图4 Main menu 菜单



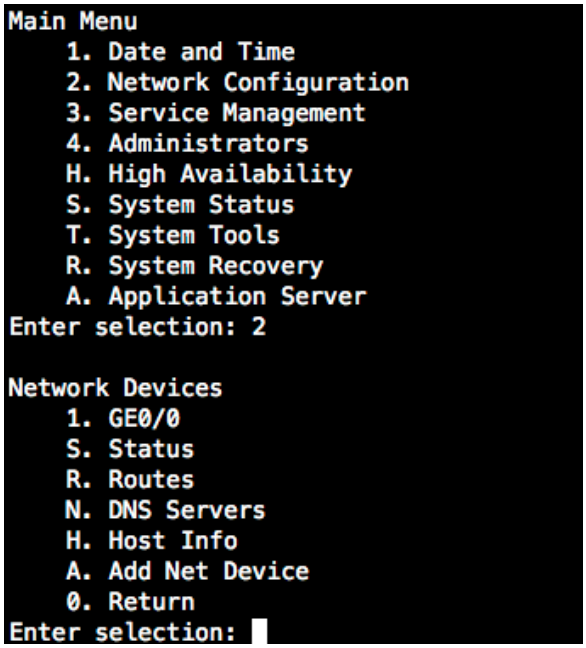
2. 配置IP地址

(1) 登录 Main menu 菜单。

按照索引选择“2”，进入“Network Configuration”。

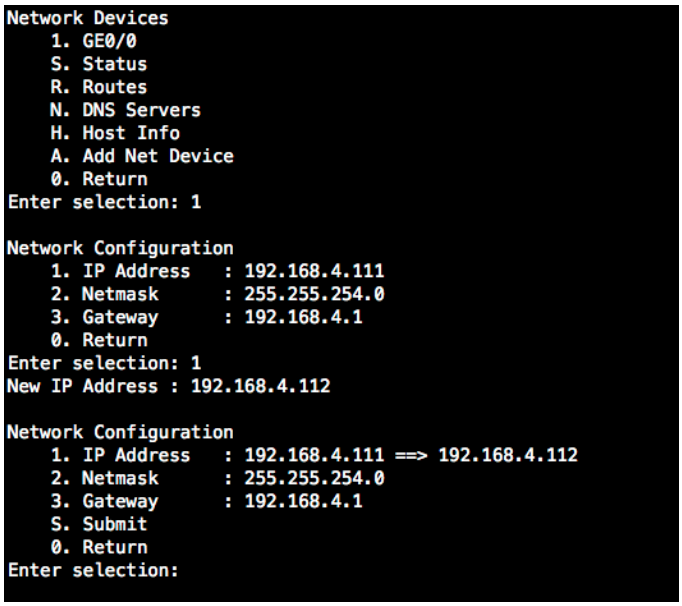
选择对应数据网口前索引，进行具体网络配置。

图5 网络配置菜单



(2) 选择相应的配置项编号即可修改该配置参数，例如：选择 1（IP Address），修改该网卡的 ip 地址，回车之后菜单中会提示您新设置的 IP 地址，确认没问题之后选择 S（submit）进行提交生效。

图6 修改 IP 地址



(3) 选择“S”提交配置更改。

3. 配置NTP(可选)

(1) 登录 Main menu 菜单。

按照索引选择“1”，进入“Date and Time”,再选择“3”，进入“Network Time Protocol”。

图7 NTP 设置

```
Main Menu
    1. Date and Time
    2. Network Configuration
    3. Service Management
    4. Administrators
    H. High Availability
    S. System Status
    T. System Tools
    R. System Recovery
    A. Application Server
Enter selection: 1

Date and Time
    1. Date : 2018-01-18
    2. Time : 15:07:52
    3. Network Time Protocol
    0. Return
Enter selection: 3
```

(2) 添加时钟服务器。

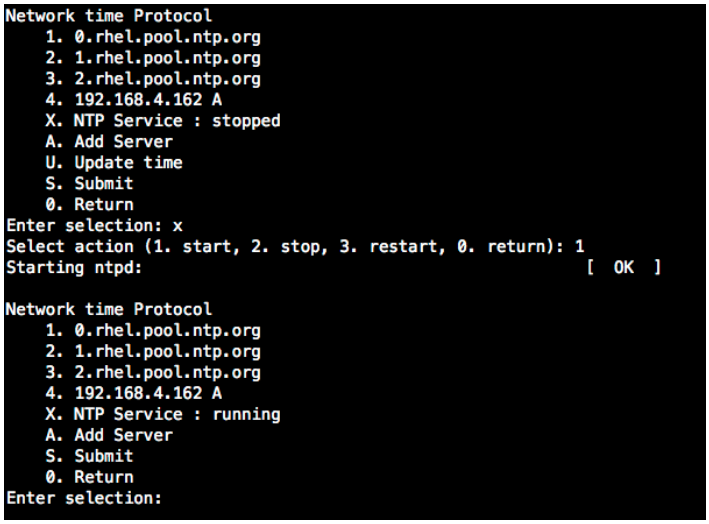
图8 添加时钟服务器

```
Network time Protocol
    1. 0.rhel.pool.ntp.org
    2. 1.rhel.pool.ntp.org
    3. 2.rhel.pool.ntp.org
    X. NTP Service : stopped
    A. Add Server
    U. Update time
    0. Return
Enter selection: a
Please input new NTP server :192.168.4.162

Network time Protocol
    1. 0.rhel.pool.ntp.org
    2. 1.rhel.pool.ntp.org
    3. 2.rhel.pool.ntp.org
    4. 192.168.4.162 A
    X. NTP Service : stopped
    A. Add Server
    U. Update time
    S. Submit
    0. Return
Enter selection:
```

(3) 启动 NTP Service 服务

图9 启动服务



说明

NTP 服务用于时间同步，如不具备配置条件，可跳过此步骤。

2.4 验证配置

使用浏览器访问配置的 IP 地址，如何通过 https://IP 可以成功登陆运维审计系统，则说明单台运维审计系统部署成功。

工单配置举例

目 录

1 简介

运维审计系统内置了工单，用于普通用户向管理员申请设备的临时访问权限。

2 配置前提

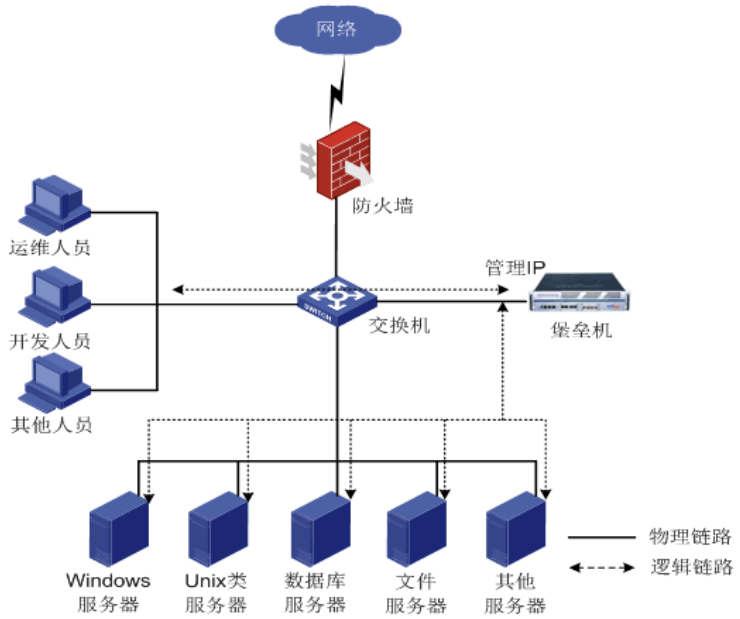
本文档不严格与具体软、硬件版本对应，如果使用过程中与产品实际情况有差异，请以设备实际情况为准。

本文档中的配置均是在实验室环境下进行的配置和验证，配置前设备的所有参数均采用出厂时的缺省配置。如果您已经对设备进行了配置，为了保证配置效果，请确认现有配置和以下举例中的配置不冲突。

3 工单配置举例

3.1 组网需求

图1 运维审计系统组网图



3.2 系统版本要求

适用产品版本：ESS 6102。

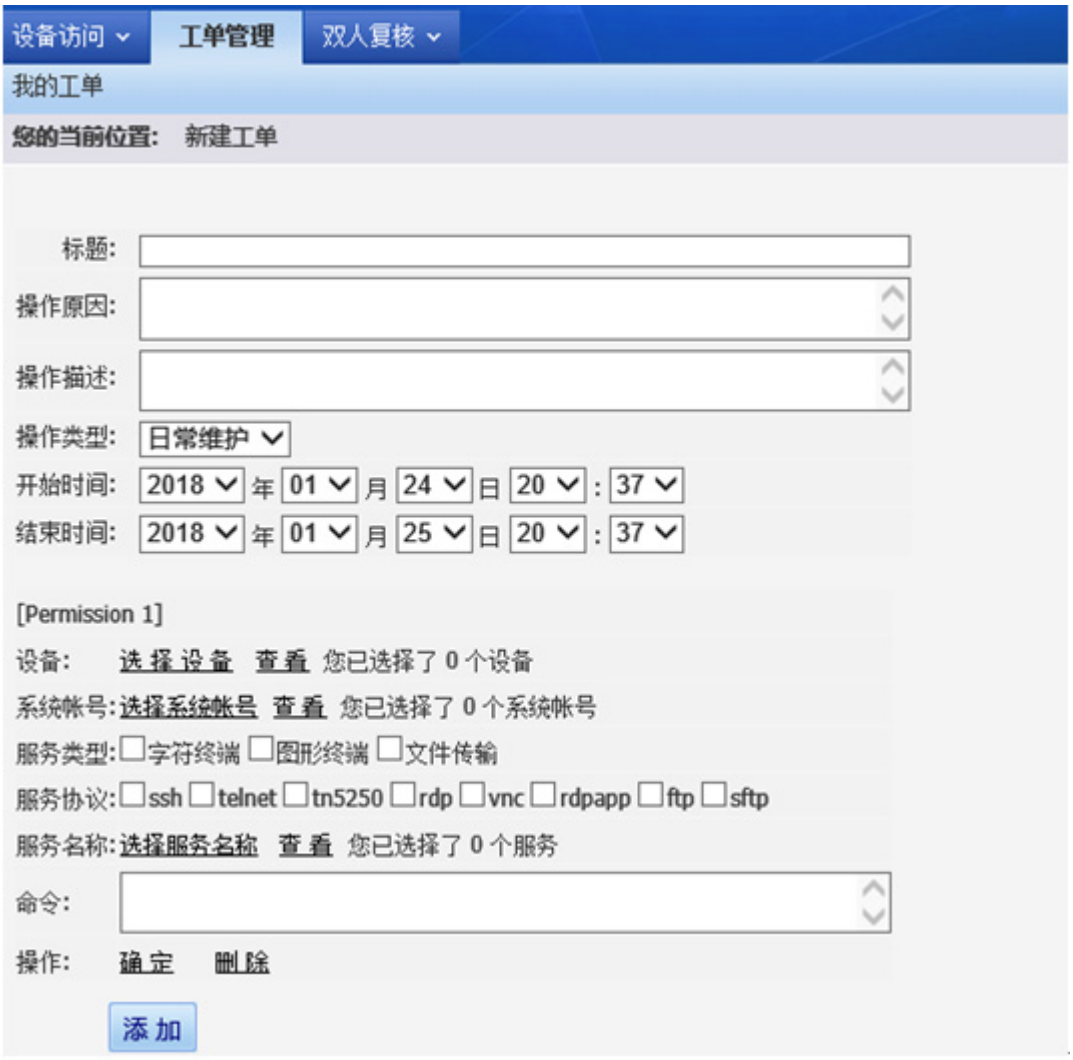
3.3 普通用户新建工单

(1) 登录 web

图2 创建工单

(2) 填写工单基本信息

图3 工单内容



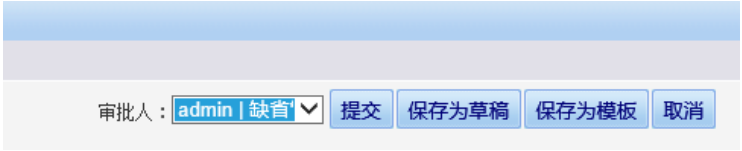
- 标题：填写所建工单的名称。
- 操作原因：工单操作的原因。
- 操作描述：操作步骤。
- 操作类型：可选“日常维护、抢修、实施、测试”。

- 时间：选择申请工单的时间段。
- Permission：
  - 设备：关联需要使用的设备。
  - 系统账号：关联需要使用的系统账号
  - 服务类型/服务协议/服务名称：关联需要使用的服务。
  - 命令：描述使用中需要执行的命令
  - 操作：确认以上填写完成后按“确定”不需要这条 permission 则按“删除”。

图4 工单任务信息

(3) 新建工单中选项填写完成后，可以选择相应配置管理员审批或者留作模板及草稿。

图5 提交工单



3.4 配置管理员审批

(1) 当普通用户管理员申请工单后，配置管理员进入 Web 页面后可在右上角看到黄色“消息”提示。

图6 消息提示

(2) 点击<消息>可看到未处理的工单。

图7 未处理的工单

	状态	类型	产生时间	简要说明	过期时间	操作
1	未读	工单	2018-01-24 20:20:47	user01: 4	2018-01-25 20:15:00	详细
2	未读	工单	2018-01-24 20:10:56	user01: 1	2018-01-25 20:09:00	详细

(3) 点击<详细>可查看当前工单主要内容，允许按<授权>，不允许则按<驳回>。

图8 处理工单

(4) 点击后页面将会提示“操作成功”，返回至[工单管理/全部工单]可查看工单当前的状态。

(5) 若有特殊情况，需要中断该工单的使用，可以点击<停用>，点击后将终止该工单的使用时限。

图9 停用工单

3.5 工单访问

3.5.1 查看可访问工单

当“配置管理审批后”，“普通用户”可登录 web 页面，打开[设备访问/工单访问]，可查看当前可以使用工单，停用或过期工单不会显示。

图10 查看可访问工单

1. 工单详细

点击相应工单<详细>，可查看该工单的描述、有效时间、可访问情况。

图11 工单详细

2. 工单访问

(1) 点击相应工单<设备访问>，进入到设备访问页面，列出可访问设备，点击服务即可访问。

图12 工单访问

说明

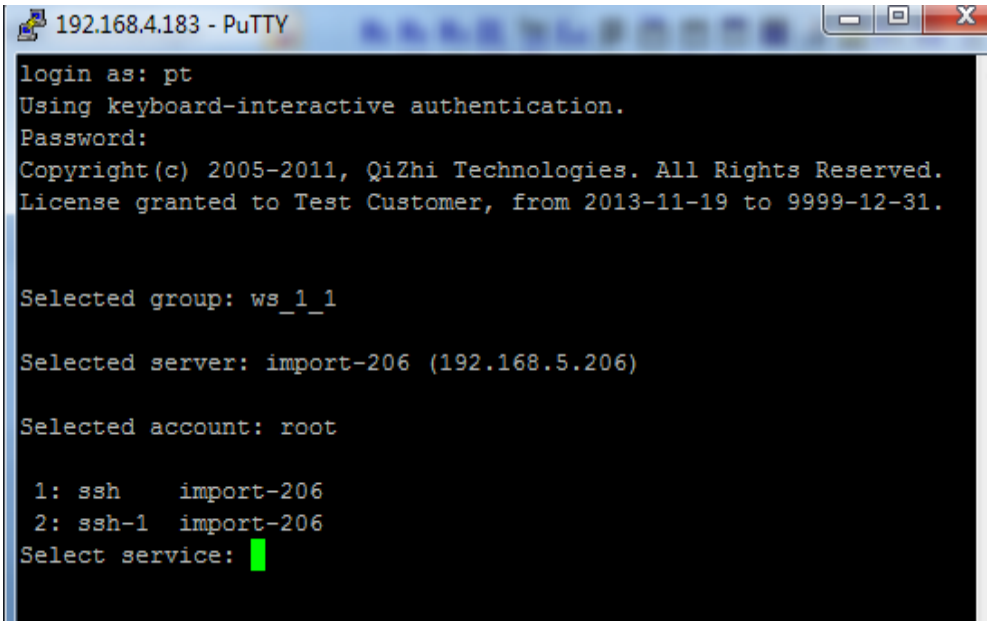
左键点击服务图标将按照上次选择的访问情况进行访问。

右键点击服务图标，将弹出高级选项窗口，手工选择分辨率、账号、磁盘映射等选项进行访问。

---

(2) 如果目标设备为字符设备，也可通过 SecureCRT、PUTTY 等工具，其中 ws_1_1 为工单生成的访问规则组，选择设备进行访问。

图13 工单访问



命令权限与命令复核配置举例

目 录

1 简介

命令权限允许配置管理员设置规则，对用户通过 ssh 和 telnet 访问时执行的命令进行匹配，并对匹配到的操作采取拒绝、切换或者告警动作。实现命令行级别的权限控制。

2 配置前提

要使用命令权限需要先了解基本的配置规则和方法

2.1 设定规则的使用范围

通过关联用户、设备和系统帐号可以设定规则的适用范围，如下图：

图1 设定规则的适用范围

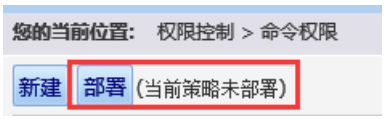
(1) 如果不关联任何用户帐号、设备和系统帐号该规则对所有用户、设备和系统帐号均有效。

(2) 如果关联了用户、设备和系统帐号规则仅对已关联的用户、设备和系统帐号有效。

2.2 使规则生效

新建或者修改规则后规则的变更不会立即生效，如下图：

图2 使规则生效



只要有“当前策略未部署”的标记存在就说明变更未生效，要使变更生效必须点击“部署”，部署后规则将在 1 分种后生效，生效后对已经存在的和新建的字符会话均有效。

2.3 命令权限的优先级

对于多条命令权限：

(1) 运维审计系统进行逐条规则匹配，执行第一条符合条件的结果，不再考虑之后的规则。

(2) 如果所有规则均不满足，按照缺省策略进行。

2.4 命令基本语法

(1) 如果不包含空格，表示只对命令部分进行匹配。

(2) 如果包含空格，第一个空格以前的部分是对命令的可执行文件部分进行匹配，与上面的规则相同；后面的部分（包括其他空格）对命令的参数部分进行匹配：就是把命令行去掉命令本身之外的所有参数部分作为一个整体，与进行匹配。

(3) 如果以"^"开头，或者包含"/"字符，表示严格匹配，即命令部分必须完全匹配正则表达式。比如"^passwd$"只匹配"passwd"本身，前面加上任何字符都认为不匹配。比如"/usr/bin/passwd$"只匹配"/usr/bin/passwd"，任何其他路径或不写路径都不接受。否则将把命令的最后一个"/"字符后的部分拿来做匹配。比如"passwd$"匹配"passwd"、"/usr/bin/passwd"、"asdf/passwd"等。

2.5 正则表达式

所有的匹配都基于正则表达式。下表为正则表达式通配符的介绍：

符号	含义
.	匹配任意字符：代表1位
^	匹配字符串的开头
$	匹配字符串的结尾
*	表示之前的模式可重复0-N次
+	表示之前的模式可重复1-N次
?	表示之前的模式可重复0-1次
{m}	表示之前的模式可重复m次
{m,n}	表示之前的模式可重复m-n次
{,n}	表示之前的模式可重复不超过n次
[...]	表示可匹配方括号内出现的任意字符，可用"-"表示范围，如a-z、0-9等
[^...]	表示可匹配方括号内未出现的任意字符，可用"-"表示范围，如a-z、0-9等
|	表示可匹配A或B，这里A和B都可以是正则表达式
\	转义符，表示取消后面字符的特殊含义，仅表示该字符本身
\d	表示可匹配任意数字字符；"\D"表示可匹配任意非数字字符
\s	表示可匹配任意空白字符；"\S"表示可匹配任意非空白字符
\w	表示可匹配任意字母、数字或下划线；"\W"表示可匹配任意非字母、数字或下划线
\r	表示回车
\n	表示换行
\t	表示制表符

2.6 Shell元字符

(1) 对于“&”和“;”可以当做普通字符处理，比如：禁止ls;cat或者top&，直接写成ls;cat或者top&。

(2) 对于“|”需要使用“/”进行转义，比如，禁止ls|xargs ls，应该写成ls/|xargs ls。

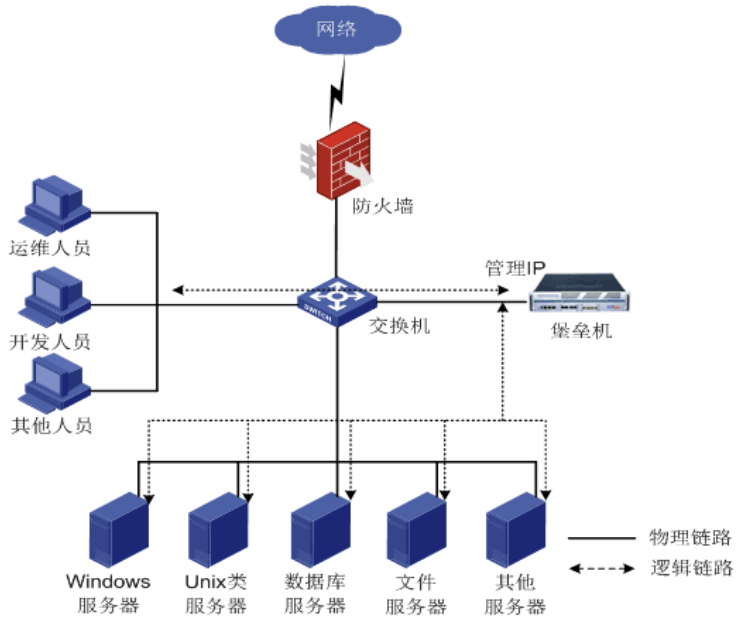
2.7 最小检查单位

运维审计系统对命令的检查是以回车符为界限进行的，只有当用户按下回车提交命令后才会执行命令权限检查。因此运维审计系统不会对shell的key binding进行检查。

3 配置举例

3.1 组网需求

图3 运维审计系统组网图



3.2 系统版本要求

适用产品版本：ESS 6102。

3.3 缺省策略为accept下的局部白名单配置举例

3.3.1 需求简介

当缺省策略为accept时，指定的用户或指定的设备只允许执行列出的指令，其余命令均被禁止执行，而其它用户或设备均采用默认策略。

3.3.2 配置过程

(1) 建任意一条动作为 accept 的权限控制策略；

(2) 建一条拒绝用户对相关设备所有操作的权限控制策略：在操作规则里填写命令.*（代表所有命令），动作为 deny，确定后再关联与上一条规则相同的用户，设备，系统帐号。

建完以上 2 规则后单击部署。如下图范例：

图4 部署策略

根据权限规则的优先级，先匹配规则 1，再匹配规则 2，最后再匹配全局缺省策略。规则 1 使用户 user01 仅可对目标设备 192.168.7.70 执行 ifconfig 和 ls 命令。虽然全局缺省策略为 accept，但因规则 2 的存在，用户 user01 对目标设备 192.168.7.70 执行其它命令时将被拒绝。

3.4 缺省策略为deny下的局部黑名单配置举例

3.4.1 需求简介

当缺省策略为 deny 时，指定的用户或指定的设备只禁止执行列出的指令，其余命令均被允许执行，而其它用户或设备均采用默认策略。

3.4.2 配置过程

(1) 建任意一条动作为 deny 的权限控制策略；

(2) 建一条允许用户对相关设备进行所有操作的权限控制策略：在操作规则里填写命令.*（.*代表所有命令），动作为 accept，确定后再关联与上一条规则相同的用户，设备，系统帐号。

建完以上 2 条规则后单击部署。如下图范例：

图5 部署策略

根据权限规则的优先级，先匹配规则 1，再匹配规则 2，最后再匹配全局缺省策略。规则 1 中使用户 user01 不可对目标设备 192.168.7.70 执行 passwd 命令。即使全局缺省策略为 deny，但因规则 2 的存在，用户 user01 可对目标设备 192.168.7.70 执行除 passwd 以外的任何命令。

3.5 命令复核配置举例

3.5.1 需求简介

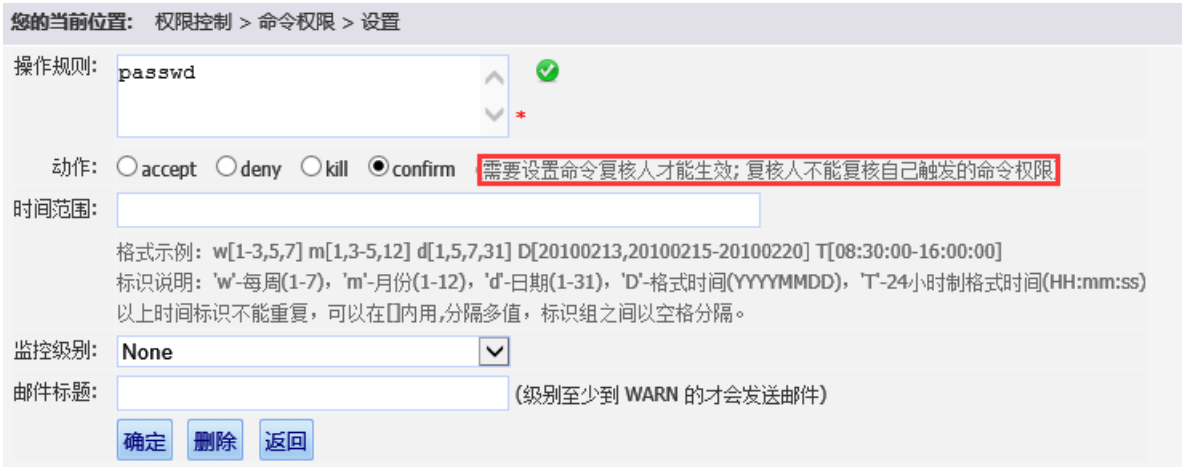
某些重要命令需要第二个人复核后才可以执行。

3.5.2 配置过程

(1) 建立动作为 confirm 的命令权限规则

触发双人复核的前提条件是设置命令的触发动作为 confirm（如图）。

图6 建立动作为 confirm 的命令权限规则



(2) 再关联上复核人即可

图7 关联上复核人

说明

触发人和复核人不能是同一人。

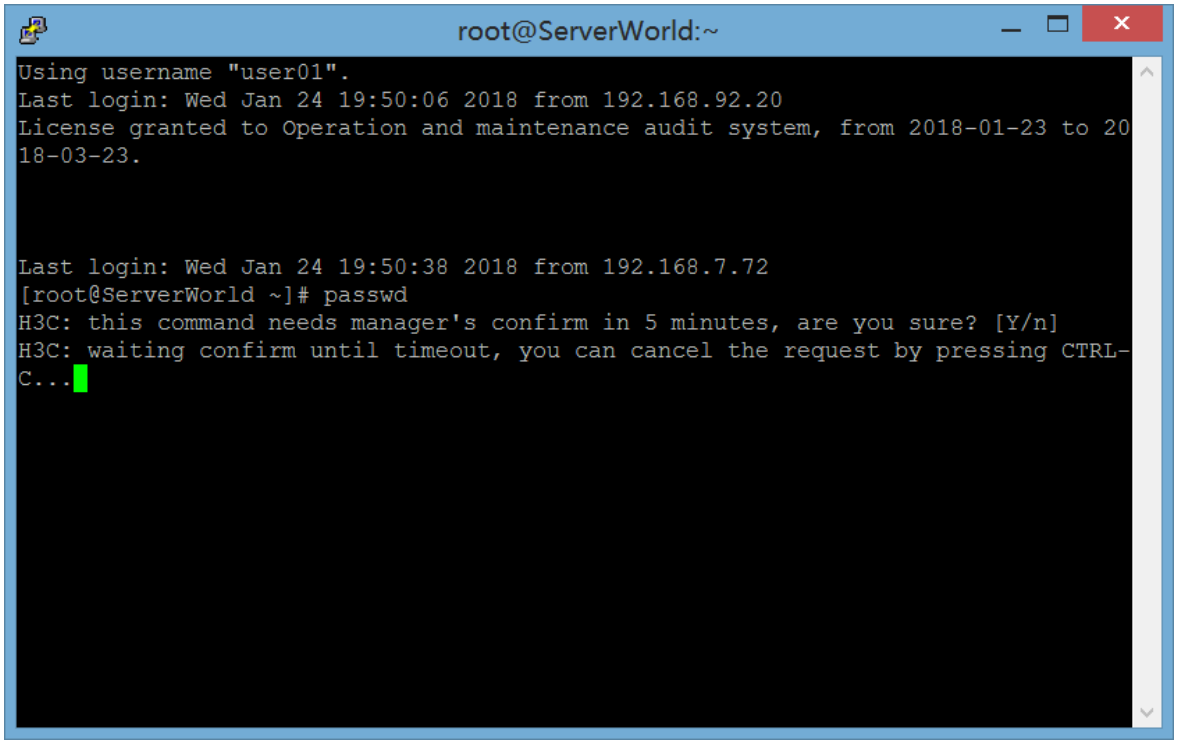
(3) 触发

当用户访问设备时，输入了我们设置的命令，会出现如下提示（如图）：

H3C：此命令需要复核人进行批准，等待超时时间为五分钟，确认请按 Y

H3C：正在等待复核人审批，直到复核人进行操作或者超时，您可以按 Ctrl+C 退出此次请求。

图8 触发



(4) 复核

同时，复核人打开“双人复核”中的“命令复核”页面中会出现提示（如图）：

图9 复核

此时存在以下操作：

- 允许：此命令正常执行。
- 拒绝：此时请求人 user01 会收到提示不被允许执行。
- 切断：将 user01 用户打开的 session 窗口关闭。

3.6 命令告警配置举例（syslog）

3.6.1 需求简介

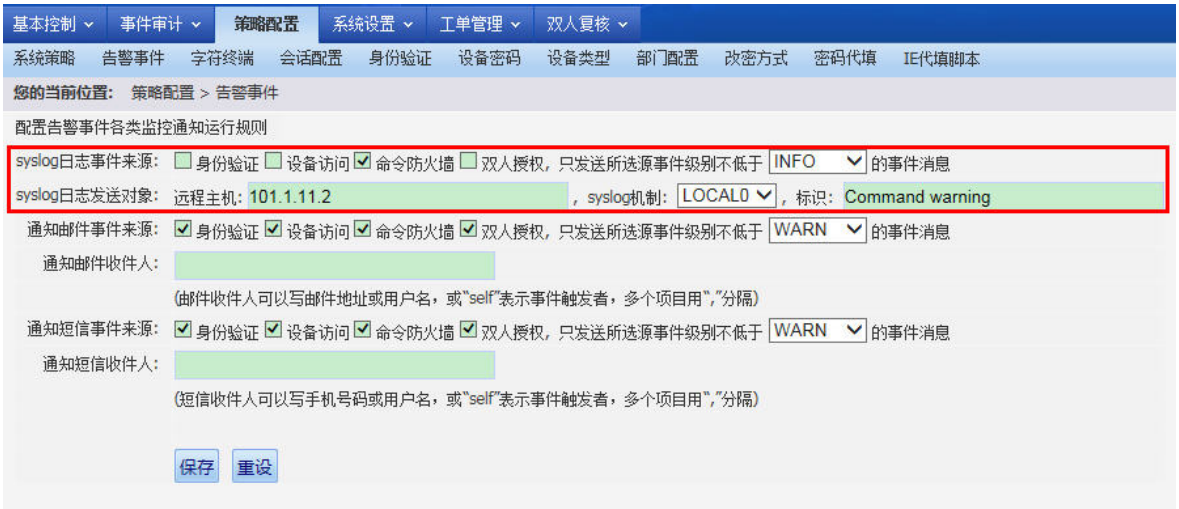
用户触发被限制的命令时，通过 syslog 方式实现告警功能。

3.6.2 配置过程

(1) 使用超级管理员登录，打开[策略配置/告警事件]页面，在 syslog 日志事件来源中勾选“命令防火墙”，只发送所选源事件级别设置为“INFO”。

(2) 在 syslog 日志发送对象的“远程主机”中填写 syslog 服务器的 IP 地址，标识填写“**Command warning**”，方便 syslog 服务器识别日志消息来源。

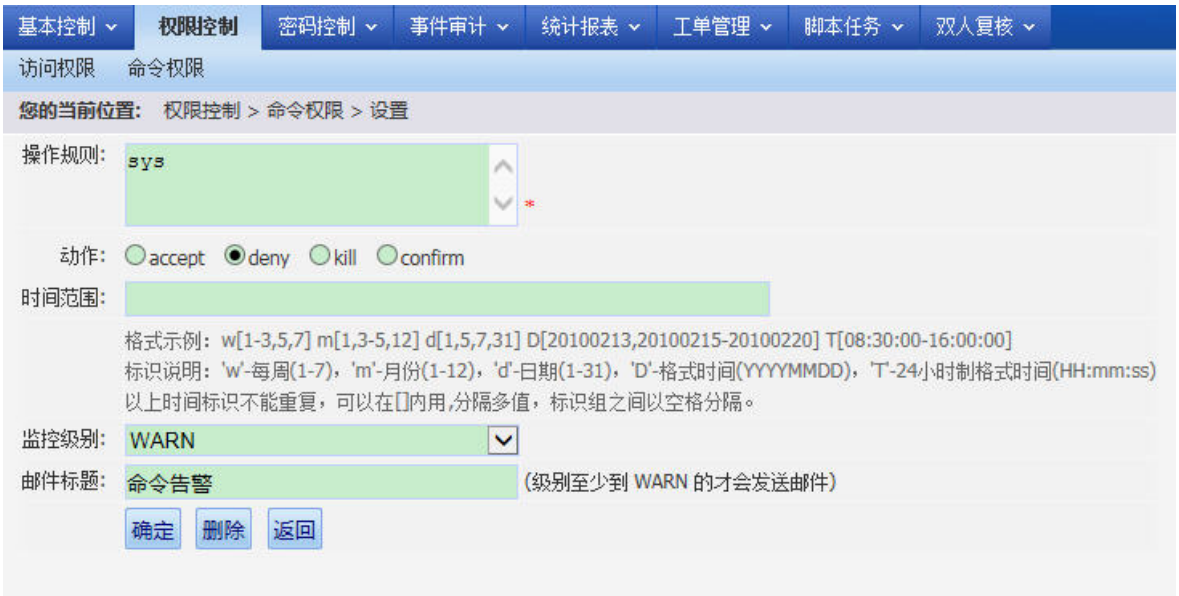
图10 配置日志信息



(3) 点击<保存>按钮。

(4) 使用配置管理员新建任意一条命令权限，监控级别设置为“WARN”，邮件标题设置为“Command warning”。

图11 权限设置



说明

监控级别设置的值要比告警级别处所设置的级别高，否则无法触发告警。

---

(5) 当用户访问设备输入了命令权限中设置的命令，就会触发告警事件。

图12 告警事件日志

```
Command warning: 命令告警(id=1498 service=cmdcheck
server=H3C_Switch(101.102.1.2) account=admin identity=admin
from=101.1.11.2 sys)
```

使用同名账户和密码登录目标设备配置举例

目 录

1 简介

使用同名账户和密码登录目标设备：是指使用运维审计系统自身的账户、密码登录目标设备。
这种方式适用于运维审计系统、目标设备上拥有同样的账户密码的情况下，在域环境下较为常见。

2 系统账户说明

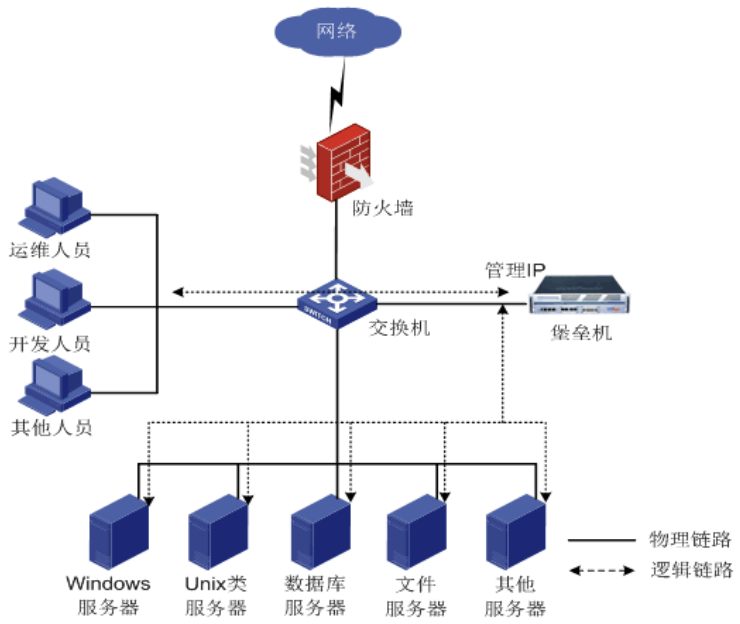
运维审计系统默认存在如下账户（使用同名账户和密码的模式主要使用的是下面的“self”账户）：

账户	说明
administrator	windows设备的默认管理账户
any	代表手工输入账户密码
enable	一般网络设备切换特权模式的命令
null	空账户，代表不输入账户名
root	linux设备默认的超级管理员
self	代表运维审计系统的同名账户

3 配置举例

3.1 组网需求

图1 运维审计系统组网图



3.2 系统版本要求

适用产品版本：ESS 6102。

3.3 AD集成配置举例

3.3.1 组网需求

拥有一台 AD 域控服务器和一台 Windows 的主机，需要将 Windows 的主机加入到 AD 域环境中。
运维审计系统采用 AD 域的认证方式。

3.3.2 配置思路

运维审计系统和需要访问的目标设备都通过 AD 域来认证。
使用“self”账号登录目标设备时，运维审计系统使用域账号密码来登录目标设备。

3.3.3 配置过程

(1) 运维审计系统增加 AD 的认证方式

登录“超级管理员”，新增 ldap 协议的认证方式。配置通过 AD 域控进行认证。

图2 增加 AD 的认证方式

(2) 新增账户，使用 AD 的认证方式

“基本控制 > 用户账号 > 新建用户”。

登录名要和 AD 上的账户一致，选择“身份验证方式”为之前配置的 AD。

ldap 用户名如果不填写，默认和登录名一致。

图3 新增账户

(3) 添加目标设备

添加目标设备，该目标设备需要是 AD 域认证，不需要托管密码。

(4) 关联访问规则

登录“配置管理员”，“权限控制 > 访问权限”。

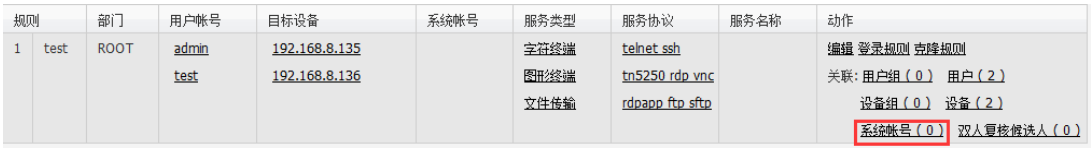
图4 关联访问规则

关联之前配置的 AD 域认证的账户，关联之前添加的目标设备。

图5 关联访问规则

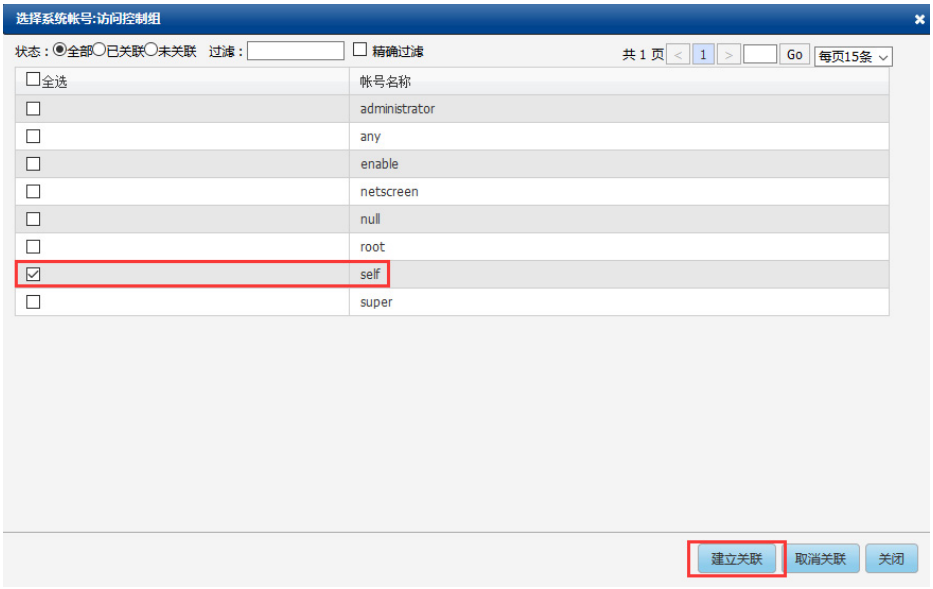
点击“系统账号”。

图6 关联访问规则



选择“self”账户，点击“建立关联”。

图7 建立关联



(5) 登录设备

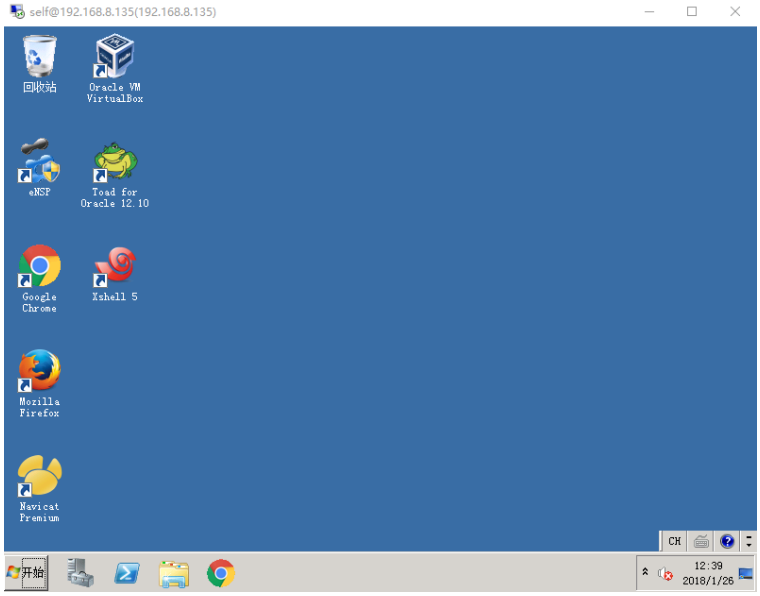
选择相应账户登录，切换到普通用户。

选择相应的目标设备，右键点击相应服务，选择“self”账户。点击确定。

图8 登录设备

直接登录进入系统。

图9 登录设备



3.4 LDAP集成配置举例

3.4.1 组网需求

(1) 拥有一台 ldap 服务器。

(2) 拥有一台 linux 的主机，并且采用 ldap 方式认证。

(3) 运维审计系统采用 ldap 的认证方式。

3.4.2 配置思路

(1) 运维审计系统和需要访问的目标设备都通过 ldap 认证。

(2) 使用“self”账号登录目标设备时，运维审计系统使用域账号密码来登录目标设备。

3.4.3 配置过程

(1) 运维审计系统增加 ldap 的认证方式。

登录“超级管理员”，新增 ldap 协议的认证方式。

图10 增加 ldap 的认证方式

(2) 新增账户，使用 ldap 的认证方式

“基本控制 > 用户账号 > 新建用户”。

登录名要和 ldap 上的账户一致，选择“身份验证方式”为之前配置的 ldap。

ldap 用户名如果不填写，默认和登录名一致。

图11 新增账户

(3) 添加目标设备

添加目标设备，该目标设备需要是 ldap 认证，不需要托管密码。

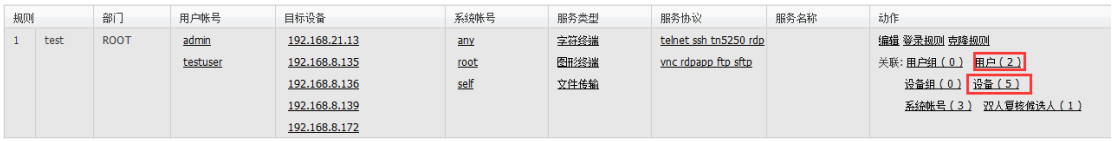
(4) 关联访问规则

登录“配置管理员”，“权限控制 > 访问权限”。

图12 关联访问规则

关联之前配置的 AD 域认证的账户，关联之前添加的目标设备。

图13 关联访问规则

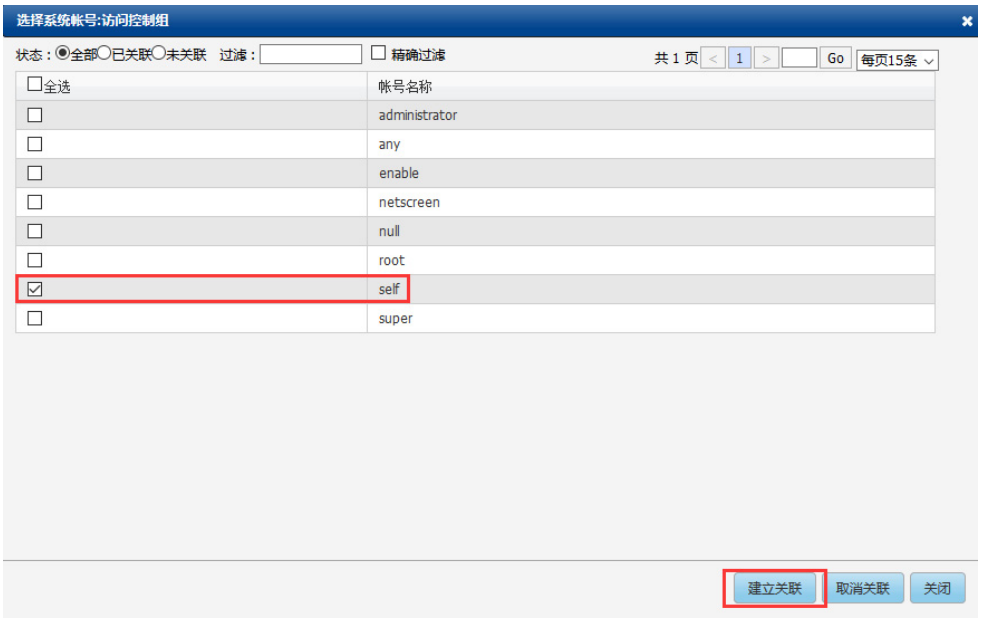


点击“系统账号”。

图14 关联访问规则

选择“self”账户，点击“建立关联”。

图15 建立关联



(5) 登录设备

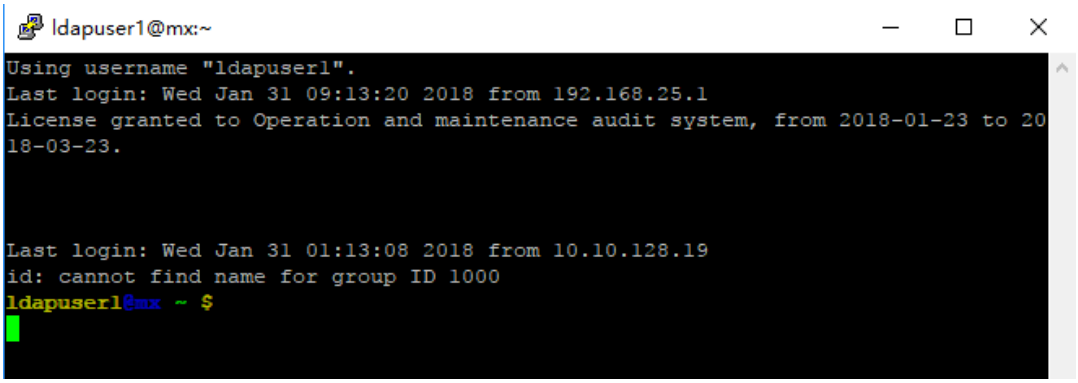
选择相应账户登录，切换到普通用户。

选择相应的目标设备，右键点击相应服务，选择“self”账户。点击确定。

图16 登录设备

直接登录进入系统。

图17 登录设备



4 常见问题

在双因素认证情况下，self 账号使用什么密码登录？

答：使用第一身份认证密码。

手机令牌（Mobile APP）配置举例

目 录

1 简介

手机令牌（TotpMobile）是基于时间的一次性密码（Totp）在手机客户端上的一次实现。依赖于种子文件和算法，通过时间戳，每 30 秒产生一个 6 位随机密码，来提供用户的登录验证服务。

运维审计系统的手机令牌功能只适用于双因素认证的场景。

2 配置前提

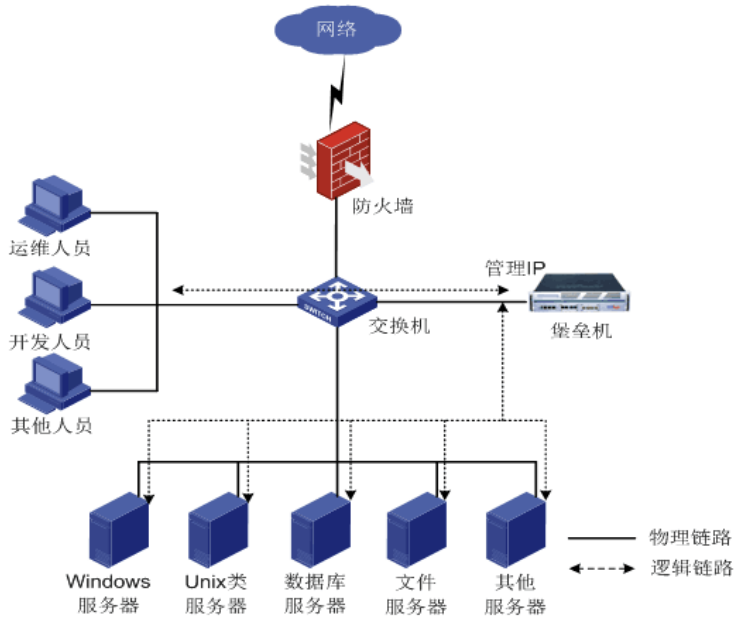
(1) 因为手机令牌与时间密切相关，所以在配置手机令牌前，请确保运维审计系统的时间与北京时间一致。

(2) 因为手机令牌与时间密切相关，所以在手机登录前，确保手机的时间和北京时间一致。

3 配置举例

3.1 组网需求

图1 运维审计系统组网图



3.2 系统版本要求

适用产品版本：ESS 6102。

3.3 创建手机令牌认证方式

登录“超级管理员”，“策略配置 > 身份验证”，选择“totp（mobile）”，点击“新建”。

图2 创建手机令牌认证方式

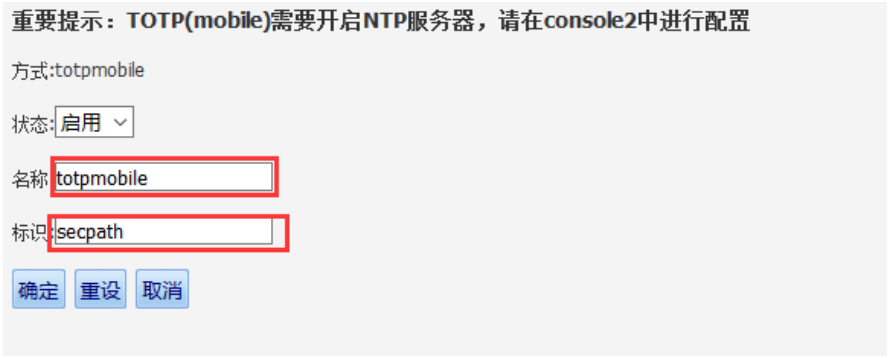
3.4 配置手机令牌认证方式

状态：选择为启用。

名称：该手机令牌认证的名称。

标识：手机 APP 上该用户的标识。（因为手机 APP 上可能存在多个账户，标识这个账户属于运维审计系统）。

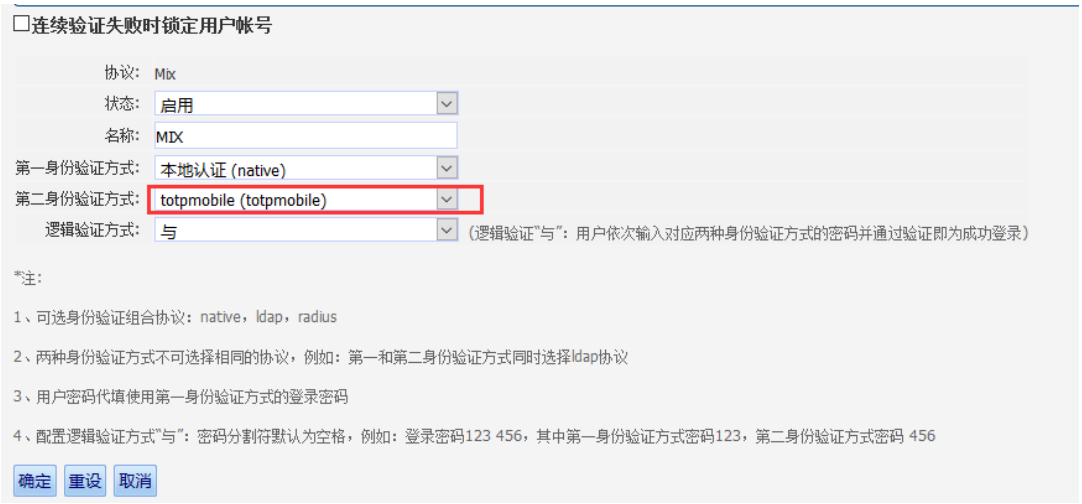
图3 配置手机令牌认证方式



3.5 配置MIX认证方式，绑定手机令牌

将第二身份验证方式选择为刚才配置的手机令牌名称。

图4 配置 MIX 认证方式



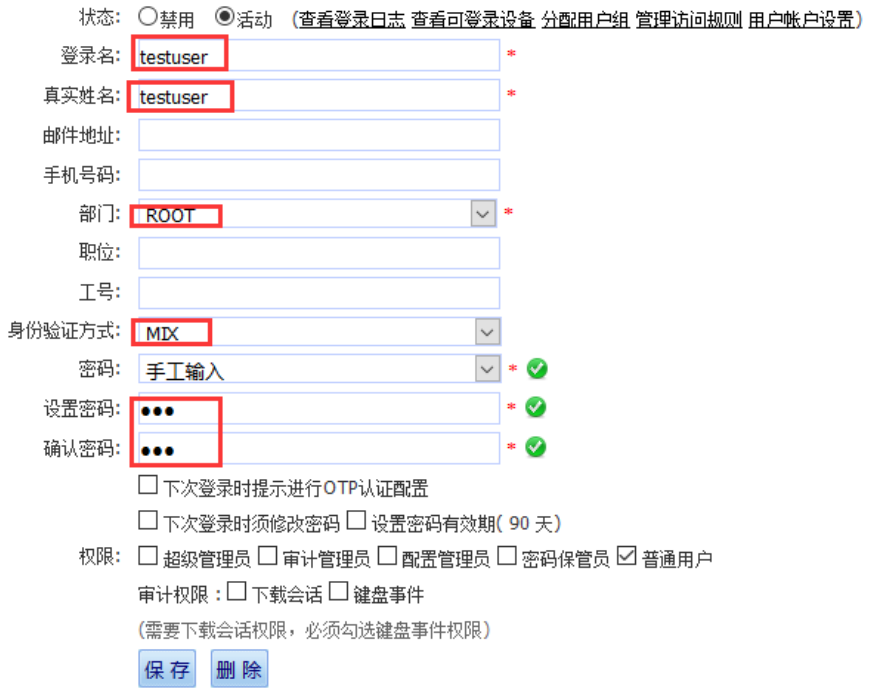
3.6 创建用户

“基本控制 > 用户账号 > 新建用户”。

图5 创建用户

- 登录名：登录运维审计系统的账户名。
- 真实姓名：该账户名的真实用户。
- 部门：选择相应的部门。
- 身份验证方式：这里选择之前配置的 mix。
- 设置密码&确认密码：这里设置第一身份验证方式的本地密码。

图6 配置用户信息



3.7 登录认证

(1) 输入账户名密码，这里的密码是第一身份验证方式的本地密码。

图7 输入账户名密码

(2) 如果是第一次登录，需要扫码完成绑定。

首先点击“Google Authenticator”，将出现下载二维码，下载手机 APP。

图8 下载手机 APP

(3) 手机 APP 扫描二维码，完成绑定操作后，点击“完成绑定”。

图9 绑定手机

(4) 输入手机 APP 产生的，相应账户、相应标识的 6 位数密码。

图10 登录

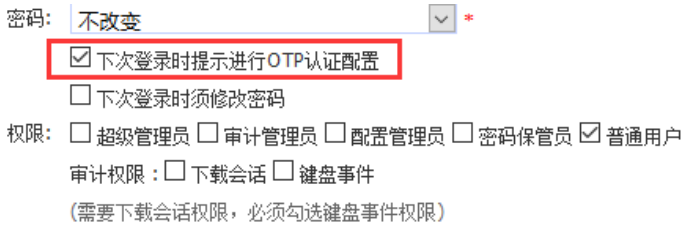
4 常见问题

(1) 为什么创建用户时，不能勾选手机令牌认证方式？

答：在运维审计系统中，手机令牌认证方式必须同其他认证方式绑定，必须是双因素认证。

(2) 如果手机丢失，或者换手机，如何重新绑定？

答：在相应用户账号中，勾选“下次登录时提示进行 OTP 认证配置”。



(3) 为什么登录老验证不成功？

答：请检查运维审计系统时间、手机时间是否与北京时间一致。

(4) 进入账户设置、rdp 直连、ssh 直连时的密码如何输入？

答：格式为，第一身份验证方式+“空格”+手机令牌密码。

双因素认证（MIX）配置举例

目 录

1 简介

双因素认证（MIX）是指，将运维审计系统已有的认证方式（本地认证、ldap 认证、radius 认证、TOTP 令牌认证、TOTPMobile 认证）两两组合的一种更高强度的认证方式。被组合的两种认证方式可以是逻辑关系上的“与”“或”关系。“与”代表两种验证方式都验证成功，才能登录成功，“或”代表两种验证方式有一种成功，就能登录成功。

2 配置前提

准备两种运维审计系统已有的认证方式。

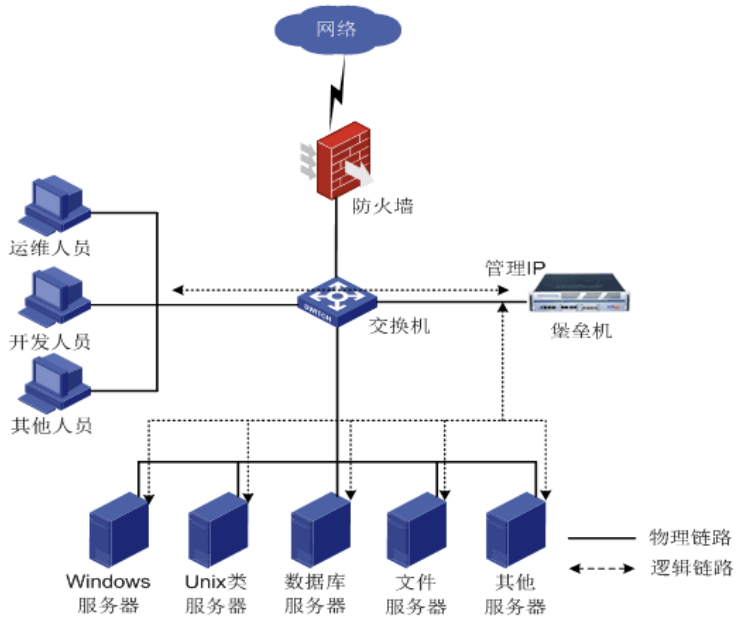
其中第一身份验证方式只能是本地认证、ldap 认证、raidus 认证其中之一。

第二身份验证方式只能是：本地认证、ldap 认证、raidus 认证、TOTPMobile 认证其中之一。

3 配置举例

3.1 组网需求

图1 运维审计系统组网图



3.2 系统版本要求

适用产品版本：ESS 6102。

3.3 创建MIX认证方式

超级管理员登录后，选择“策略配置 > 身份验证”。

图2 创建 MIX 认证方式

选择“协议”为“双因素组合（MIX）”，点击新建。

图3 选择协议

3.4 编辑MIX认证方式

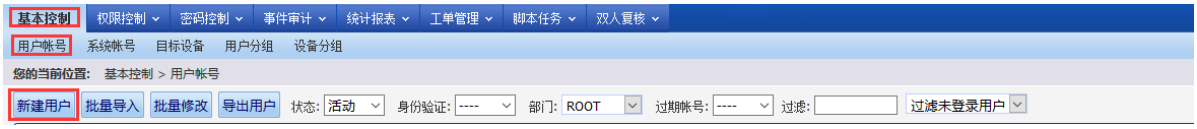
- 状态：选择为“启用”。
- 名称：给当前 MIX 认证取名。
- 第一身份认证方式：这里选择本地认证。
- 第二身份认证方式：这里选择之前配置的 ldap。
- 逻辑验证方式：这里选择“与”的关系，两个身份验证都通过则登录成功。

图4 编辑 MIX 认证方式

3.5 创建用户，绑定MIX认证方式

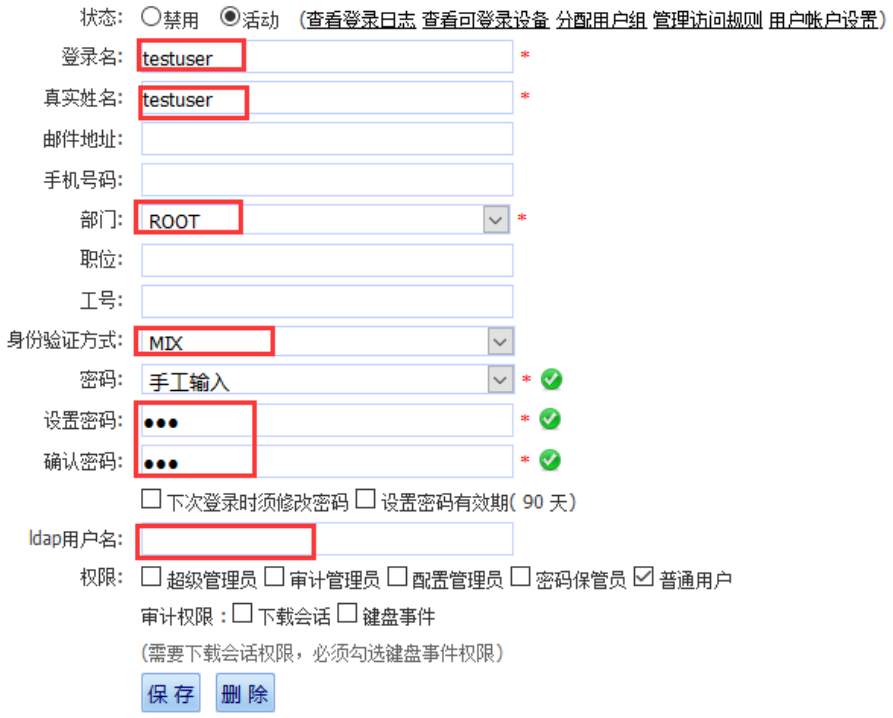
“基本控制 > 用户账号”，点击“新建用户”。

图5 创建用户



- 登录名：登录运维审计系统的账户名。
- 真实姓名：该账户名的真实用户。
- 部门：选择相应的部门。
- 身份验证方式：这里选择之前配置的 mix。
- 设置密码&确认密码：这里设置第一身份验证方式的本地密码。
- ldap 用户名：绑定该登录名对应的 ldap 账户，如果不填，则默认此项为登录名。

图6 配置用户信息

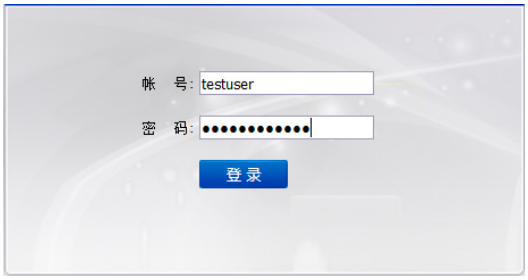


3.6 登录认证

密码部分填写 MIX 认证的双因素密码。

格式为：“第一验证密码”+“空格”+“第二验证密码”。

图7 登录设备



文件传输配置举例

目 录

1 简介

1.1 文件传输方式

运维审计系统传输文件的方式很多，根据目标设备的不同主要有两大类：

(1) Windows：

rdp 方式、ftp 方式。

(2) Linux 和类 UNIX：

rzsz 方式、sftp/scp 方式（仅 OpenSSH）、ftp 方式（仅 vsftpd）。

推荐在 Windows 环境下使用 rdp 方式；在 Linux 和类 UNIX 环境下使用 rzsz 方式。

Sftp、ftp 和 scp 的服务器及客户端环境配置复杂且存在存在兼容性问题，不推荐使用。

1.2 文件传输客户端和服务端

运维审计系统对文件传输的客户端和服务端的使用要求请参见如下两个表格

表1 文件传输客户端

客户端	使用备注
scp命令	scp 1.txt user@shtermip:/serverip/account/var/testdir
FileZilla客户端	WEB页面访问/客户端直连
WinSCP客户端	客户端直连
zmodem	SecureCRT/Xshell进行文件传输
rdp	rdp进行复制/粘贴文件

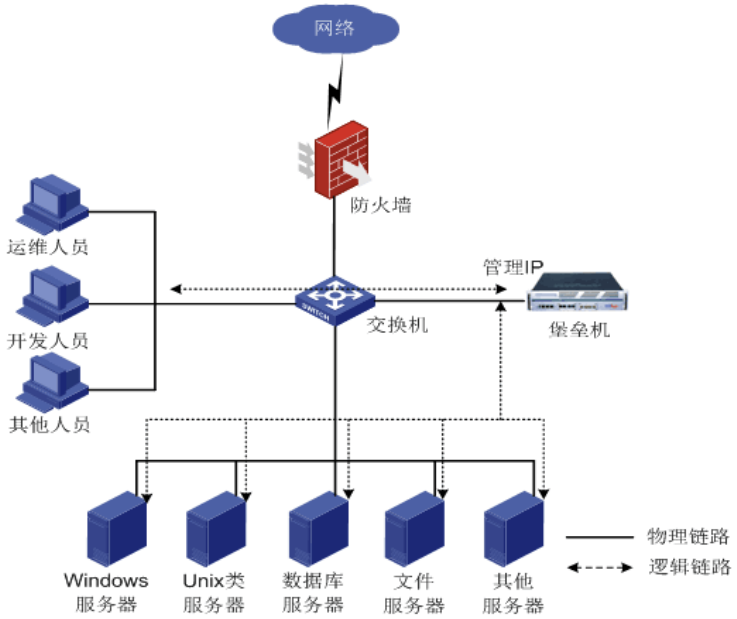
表2 文件传输服务端

服务端	FTP 服务/软件
Linux/Unix ftp	vsftpd
Linux/Unix sftp	openssh
Windows ftp	IIS自带的FTP（目录浏览样式设置为UNIX）

2 配置举例

2.1 组网需求

图1 文件传输配置组网图



2.2 系统版本要求

适用产品版本：ESS 6102。

2.3 Windows磁盘映射文件传输配置举例

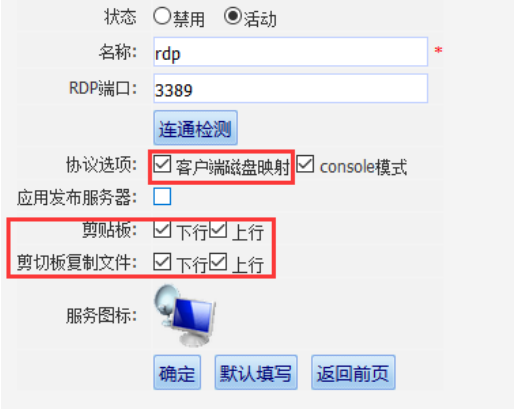
2.3.1 管理员启用RDP磁盘映射

进入“配置管理员”，“基本控制 > 目标设备”。

选择相应的 windows 设备，点击“编辑”，进入“服务列表”，编辑 rdp 服务。

勾选“客户端磁盘映射”，勾选剪切板相关的配置。

图2 编辑 rdp 服务

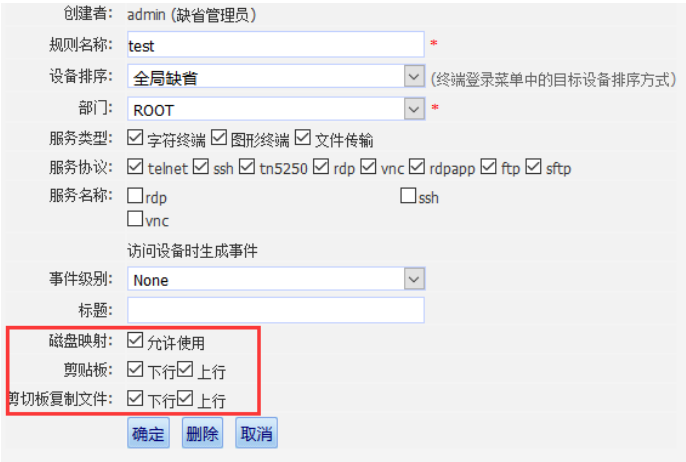


进入“配置管理员”，“权限控制 > 访问权限”。

选择相应访问规则，点击“编辑”。

勾选“磁盘映射”，勾选剪切板相应选项。

图3 编辑访问规则



2.3.2 普通用户使用方法

进入“普通用户”。

选择相应设备的 RDP 服务，右键点击。

勾选需要映射的磁盘。

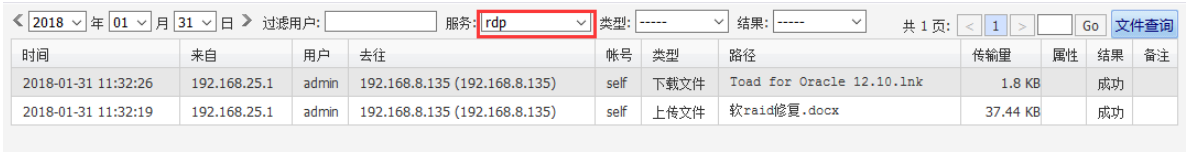
图4 普通用户使用方法

2.3.3 审计管理员查看审计记录

进入“审计管理员”，“会话审计 > 文件传输”。

通过服务过滤 rdp 服务。

图5 审计管理员查看审计记录



2.4 Linux/Unix rz/sz文件传输配置举例

2.4.1 配置前提

目标 linux 设备安装有 lrzsz 的包。

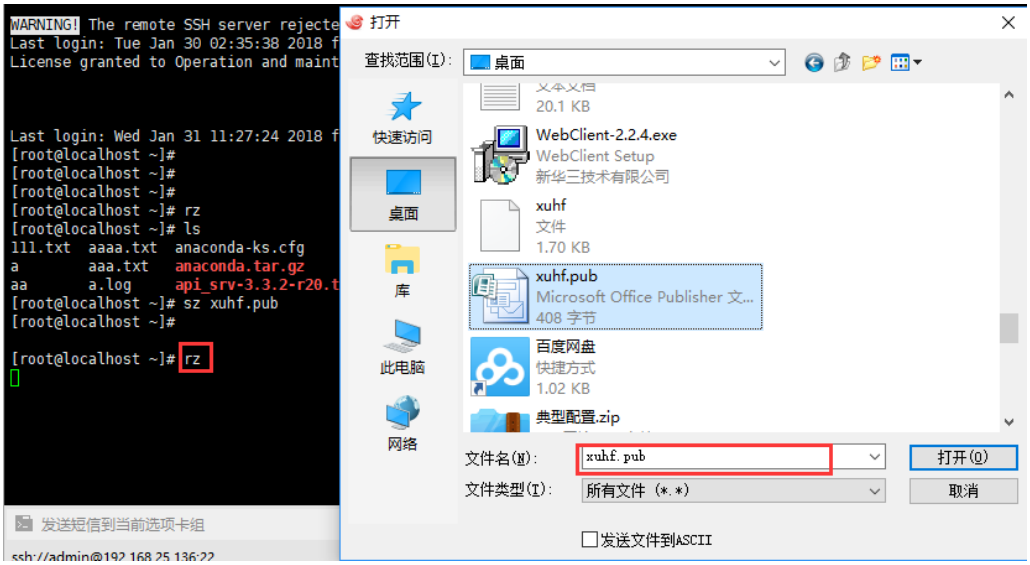
本地 PC 需要有支持 ZModem 的 SSH 客户端。

2.4.2 上传和下载

通过运维审计系统访问目标设备。

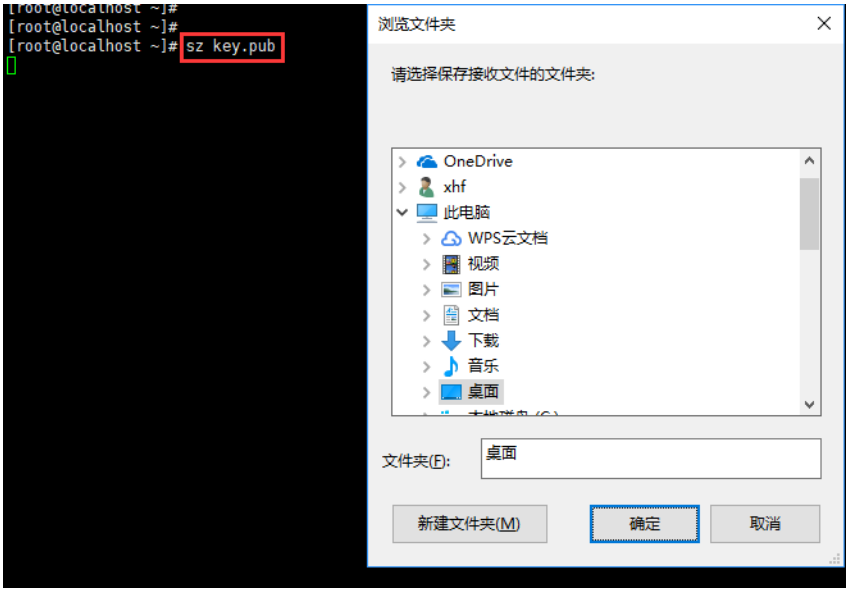
输入“rz”命令，进行文件上传。

图6 上传文件



输入“sz 文件名”，进行文件下载。

图7 下载文件

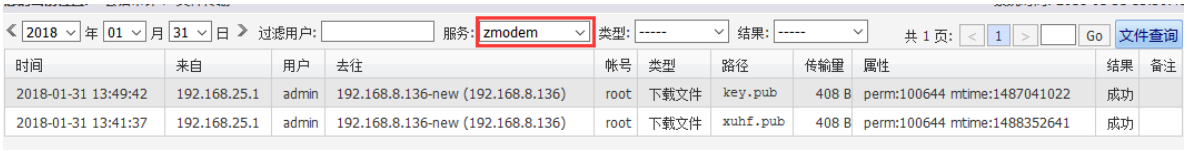


2.4.3 审计

进入“审计管理员”，“会话审计 > 文件传输”。

通过服务过滤 zmodem 服务。

图8 审计



2.5 Linux/Unix sftp/scp 文件传输配置举例（不推荐）

2.5.1 配置前提

sftp 和 scp 都依赖于目标设备提供 sshd 服务。

使用 sftp 需要本地 PC 拥有 filezilla 软件。

2.5.2 管理员启用sftp服务

1. 仅个别设备开启

进入“配置管理员”，“基本控制 > 目标设备”。

选择相应设备，进入“服务列表”，增加 sftp 服务。

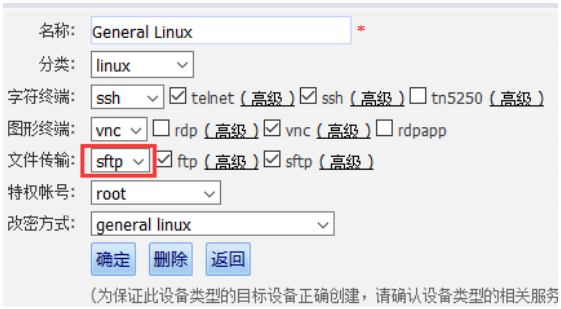
图9 增加 sftp 服务

2. 特定设备类型默认开启

进入“超级管理员”，“策略配置”-“设备类型”。

选择需要默认开启的设备类型，点击“管理”，新增默认文件传输方式为 sftp。

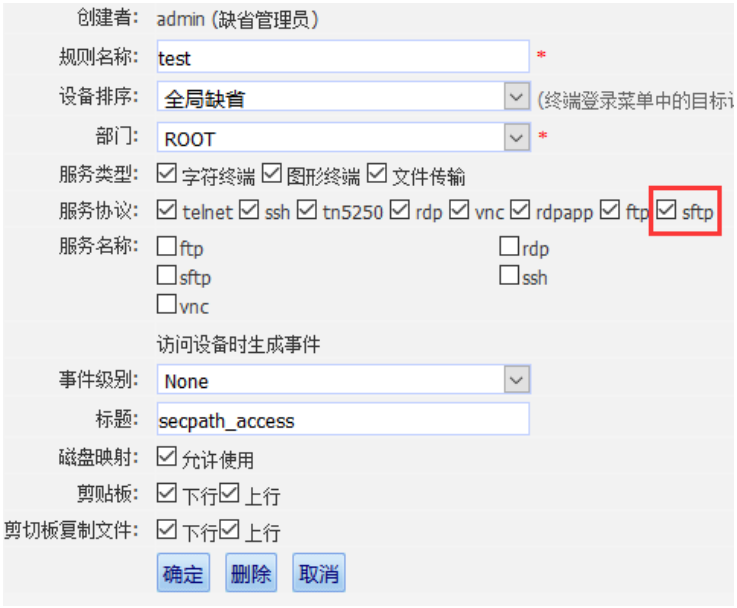
图10 选择需要默认开启的设备类型



进入“配置管理员”，“权限控制 > 访问权限”。

选择相应的访问规则，点击“编辑”，勾选 sftp 服务。

图11 选择 sftp 服务



2.5.3 普通用户访问

1. Web页面启动filezilla

进入“普通用户”，选择相应设备，右键点击 sftp 服务。

- 托管密码方式

系统账户，选择已经托管密码的系统账户（前面有个*）。

图12 托管密码方式

- 不托管密码方式

系统账户，选择 any 账户。输入用户名、密码。

图13 不托管密码方式

2. Filezilla直连

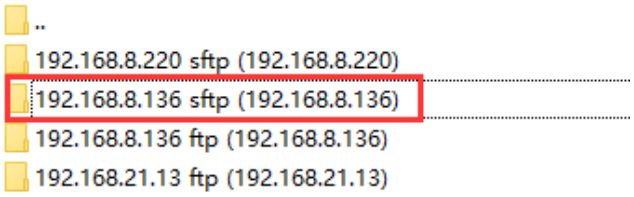
(1) 打开本地 PC 的 filezilla 软件。

- 主机格式为：sftp://运维审计系统 IP
- 用户名：运维审计系统普通用户账户名。
- 密码：运维审计系统普通用户密码。

图14 Filezilla 直连

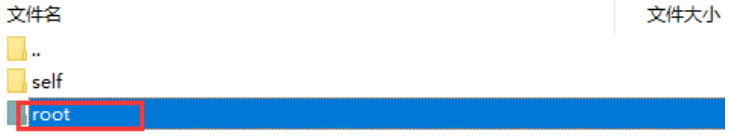
(2) 选择目标设备。

图15 选择目标设备



(3) 选择目标设备的系统账户（该账户必须在运维审计系统托管了账户密码）。

图16 选择目标设备的系统账户



(4) 列出目标设备的目录。

图17 列出目标设备的目录

文件名	文件大小	文件类型	最近修改	权限	所有者/组
..					
.autofsck	0	AUTOFSC...	2017/12/13 8:47:12	-rw-r--r--	root root
111.txt	28	文本文档	2016/11/16 12:05:52	-rw-r--r--	root root
.autorelabel	0	AUTOREL...	2016/6/17 9:36:53	-rw-r--r--	root root
root		文件夹	2018/1/31 14:10:11	dr-xr-x---	root root
tmp		文件夹	2018/1/31 3:27:02	drwxrwxrwt	root root
etc		文件夹	2018/1/26 12:48:28	drwxr-xr-x	root root
home		文件夹	2018/1/19 10:01:50	drwxr-xr-x	root root
dev		文件夹	2017/12/13 8:47:19	drwxr-xr-x	root root
sys		文件夹	2017/12/13 8:47:09	drwxr-xr-x	root root
proc		文件夹	2017/12/13 8:47:09	dr-xr-xr-x	root root
media		文件夹	2017/12/12 18:49:30	drwxr-xr-x	root root

3. scp

支持 scp 命令的客户端可以直接将本地文件，通过运维审计系统发送至目标设备。

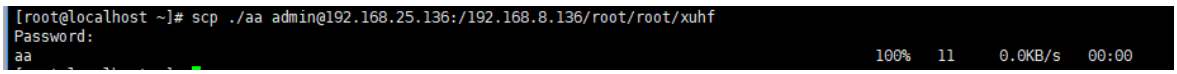
scp 的格式为：

scp 文件名 运维审计系统用户账号@运维审计系统主机地址:/目标设备地址/ftp 帐户/目标设备目录

如果 admin（用户帐户）要通过运维审计系统（192.168.25.136）使用 root 账户，将本机的 aa 文件上传到目标设备（192.168.8.136）的/root/xuhf 目录中，可以使用如下命令：

scp ./aa admin@192.168.25.136:/192.168.8.136/root/root/xuhf

- 运维审计系统用户账号为：admin
- 运维审计系统的主机地址为：192.168.25.136
- 目标设备地址为：192.168.8.136
- 目标设备的 sftp 帐户为：root
- 相应工作目录为 root/xuhf



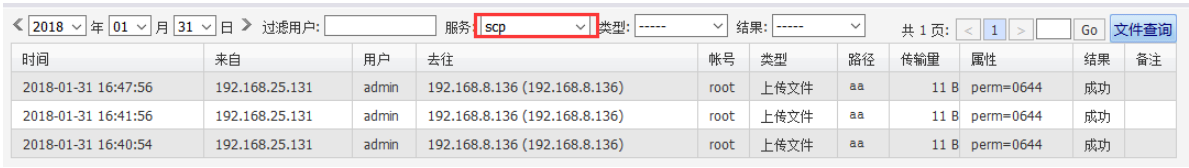
```
[root@localhost ~]# scp ./aa admin@192.168.25.136:/192.168.8.136/root/root/xuhf
Password:
aa                                                    100%   11     0.0KB/s   00:00
```

2.5.4 审计

进入“审计管理员”，“会话审计 > 文件传输”。

通过服务过滤 sftp/scp 服务。

图18 审计



2018 年 01 月 31 日 过滤用户: 服务: scp 类型: ----- 结果: ----- 共 1 页: 1 Go 文件查询

时间	来自	用户	去往	帐号	类型	路径	传输量	属性	结果	备注
2018-01-31 16:47:56	192.168.25.131	admin	192.168.8.136 (192.168.8.136)	root	上传文件	aa	11 B	perm=0644	成功	
2018-01-31 16:41:56	192.168.25.131	admin	192.168.8.136 (192.168.8.136)	root	上传文件	aa	11 B	perm=0644	成功	
2018-01-31 16:40:54	192.168.25.131	admin	192.168.8.136 (192.168.8.136)	root	上传文件	aa	11 B	perm=0644	成功	

应用发布配置举例

目 录

1 应用中心介绍

应用中心由 windows server 2008 服务器平台搭建的。

应用中心用于安装应用程序，并能通过 RemoteApp 服务发布应用程序。

1.1 支持Windows server 2008的版本

Windows Server 2008 Standard

Windows Server 2008 Enterprise

Windows Server 2008 Datacenter

1.2 RemoteApp应用发布介绍

RemoteApp 是微软在 Windows Server 2008 之后，在其系统中集成的一项服务功能，使用户可以通过远程桌面访问远端的桌面与程序，客户端本机无须安装应用程序的情况下也能正常使用远端发布的各种的桌面与应用。

1.3 RemoteApp对终端的要求

由于是采用 RDP 协议访问应用中心提供的应用程序，所以对终端平台有以下要求：

(1) 终端操作系统必须为 windows 操作系统。

(2) windows 的 RDP 版本至少 6.1 版本。

(3) 如果终端操作系统为 windows XP，请检查 RDP 版本，如果版本过低请升级 RDP 版本。

1.4 应用中心授权许可介绍

应用中心授权许可证是用于对 windows server 2008 的远程桌面服务（RDS）进行授权许可，只有正确 RDS 授权许可成功之后，运维审计系统访问应用中心的远程桌面服务就没有时间限制；未进行 RDS 授权许可的应用中心只有 120 天的使用有效期。

2 配置前提

2.1 安装前准备

2.1.1 硬件配置

堡垒机对于应用发布服务器的硬件配置需求取决于访问应用发布会话的并发数，以及各应用程序所需要消耗系统资源的多少，推荐的配置如下表所示：

表1 推荐的硬件配置

硬件	需求
处理器	最低：双核CPU
内存	最低：8GB RAM
可用磁盘空间	最低：100GB

2.1.2 操作系统

1. 版本

Microsoft Windows Server 2008 R2

2. 补丁

由于 Windows Server 2008 R2 的 bug，使用 RemoteApp 过程中可能会出现“由于协议错误，会话将被中断。请重新连接到远程计算机”，因此请务必保证应用发布服务器为 Windows Server 2008 R2，并安装 sp1 补丁，然后安装 Windows6.1-KB2696020-x64.msu、Windows6.1-KB2699817-x64.msu、Windows6.1-KB2798286-x64.msu 三个补丁。

SP1 补丁请从这里下载：http://support.microsoft.com/kb/976932。

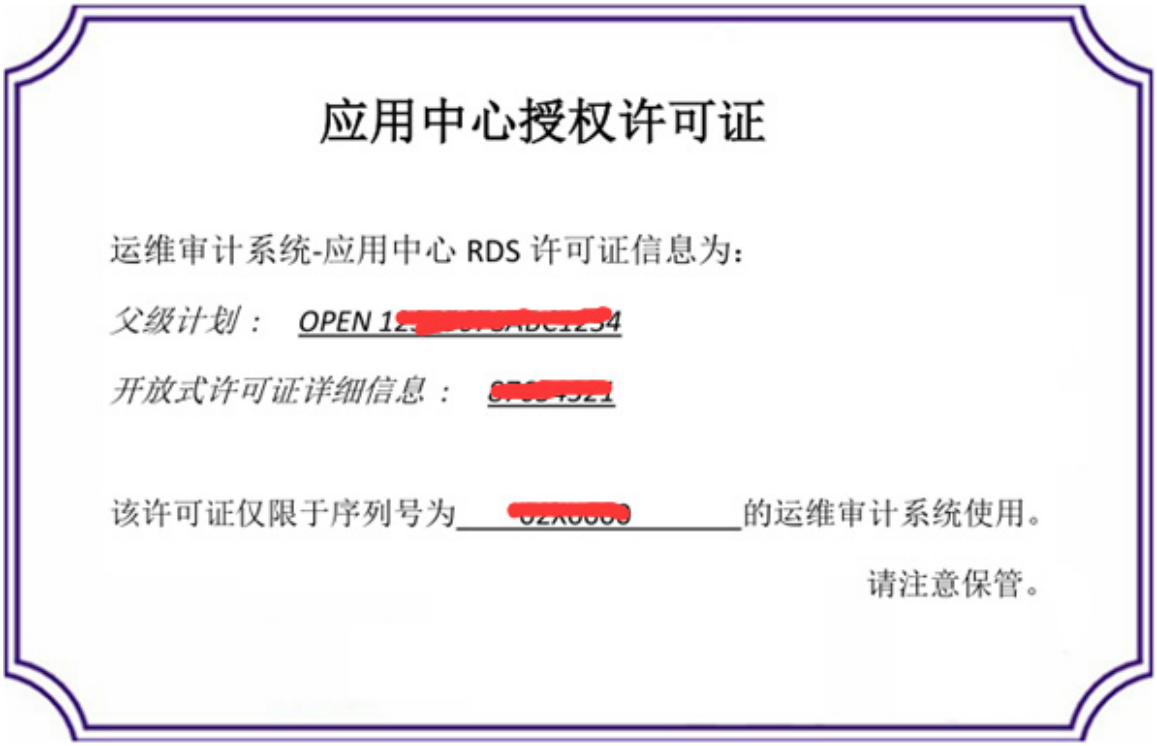
2.1.3 网络

堡垒机到应用发布服务器之间网络不要做限制，并且保证应用发布服务器上所安装的客户端能正常访问服务端。

2.1.4 RDS授权码

想要长期使用应用中心，须配备一套 RDS 授权码。如下图：

图1 RDS 授权码示意图



注意

示意图中的“父级计划”号码和“开放式许可证详细信息”号码是一组无效的示例号码；请勿使用！否则应用中心授权失败。

RDS 授权码可以向运维审计系统供应商采购，也可以直接向微软销售渠道采购。

默认 windows 的 RDS 安装好之后，有 120 天的有效试用期，足以满足测试试用。

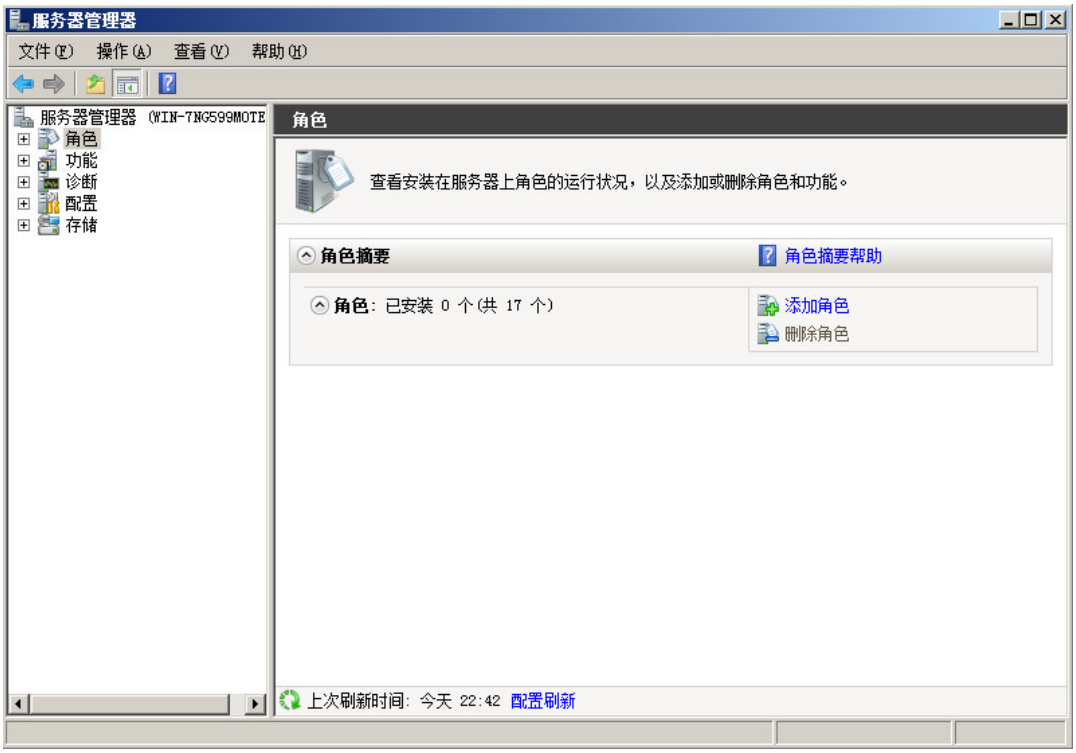
3 应用发布服务器配置准备

本章节以 Windows Server 2008 R2 Enterprise 的配置为例。

3.1 安装远程桌面服务（必配步骤）

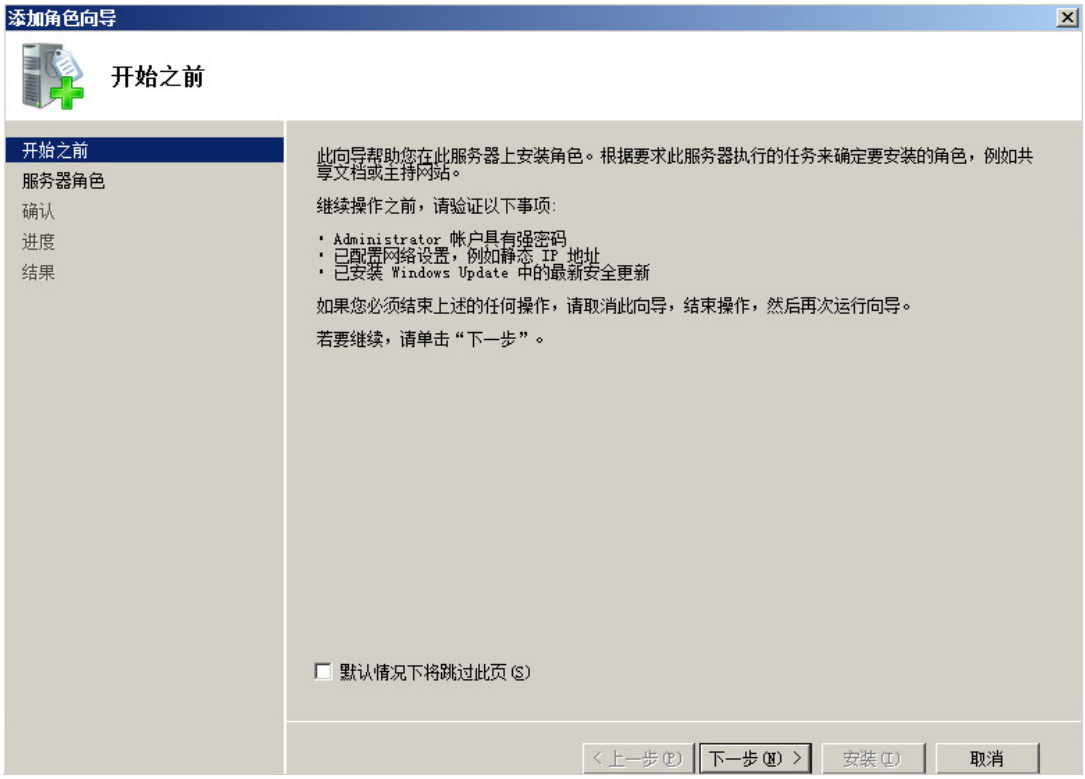
(1) 在 windows server 2008 系统中，进入[服务器管理器/角色]窗口。

图2 服务器管理器示意图



(2) 单击<添加角色>，进入添加角色向导窗口。

图3 添加角色向导示意图



(3)　单击<下一步>进入选择服务器角色窗口，勾选“远程桌面服务”。

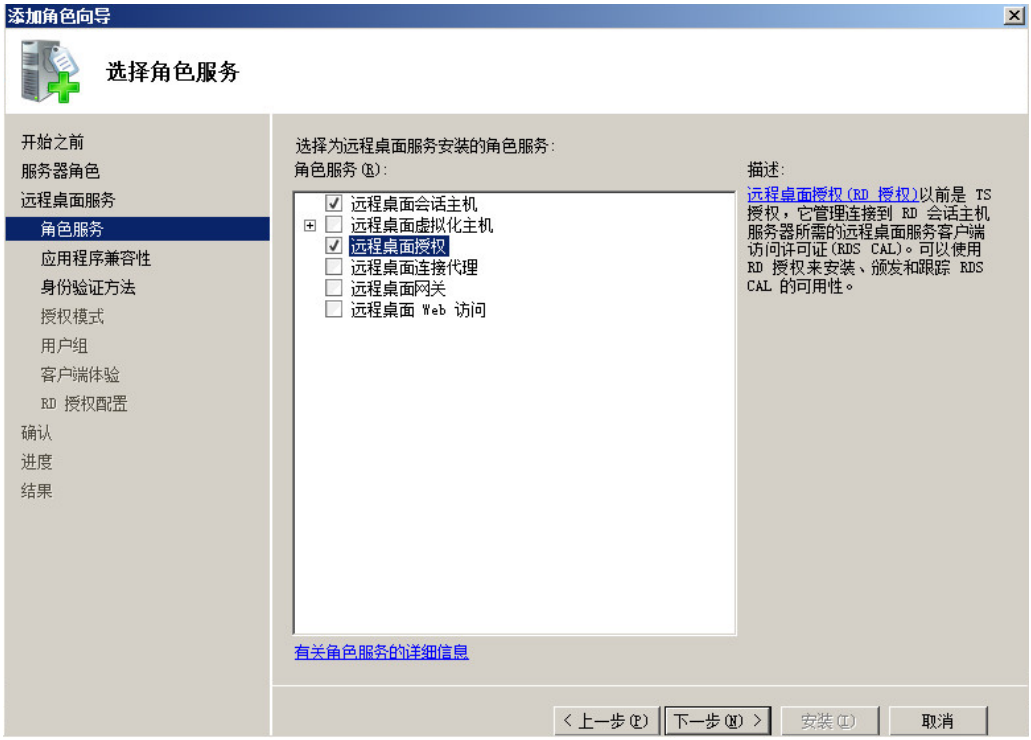
图4 选择服务器角色示意图

(4)　单击<下一步>进入远程桌面服务窗口。

图5 远程桌面服务简介示意图

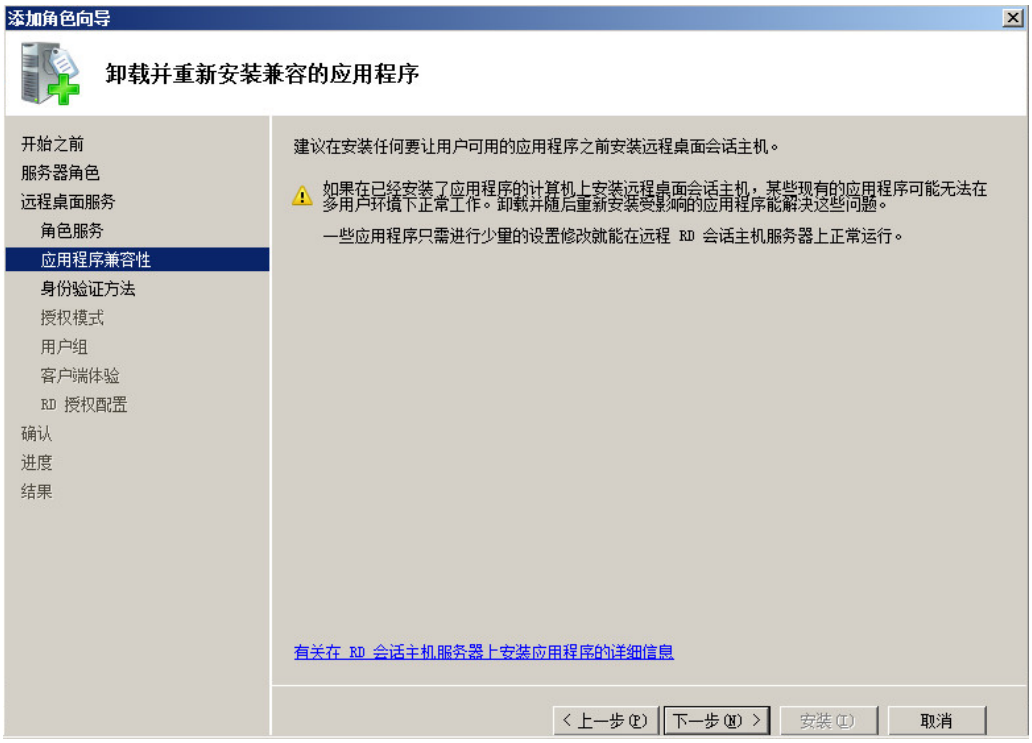
(5)　单击<下一步>进入选择角色服务窗口，勾选“远程桌面会话主机”和“远程桌面授权”服务。

图6 选择角色服务示意图



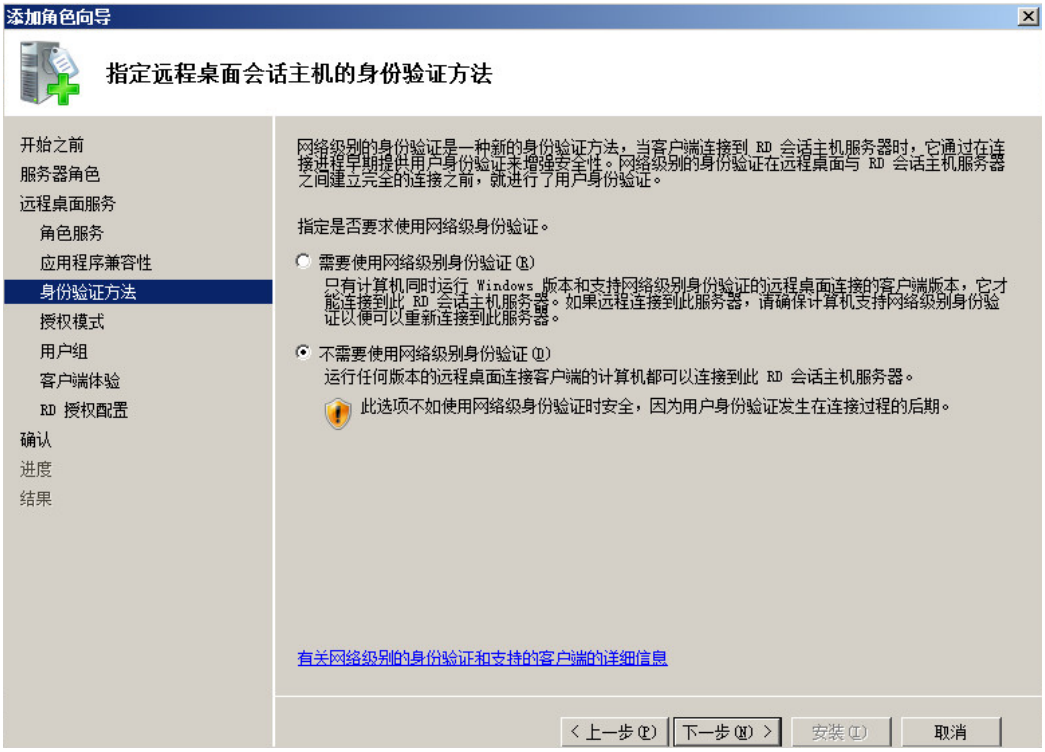
(6)　单击<下一步>进入应用程序兼容性窗口。

图7 应用程序兼容性提示示意图



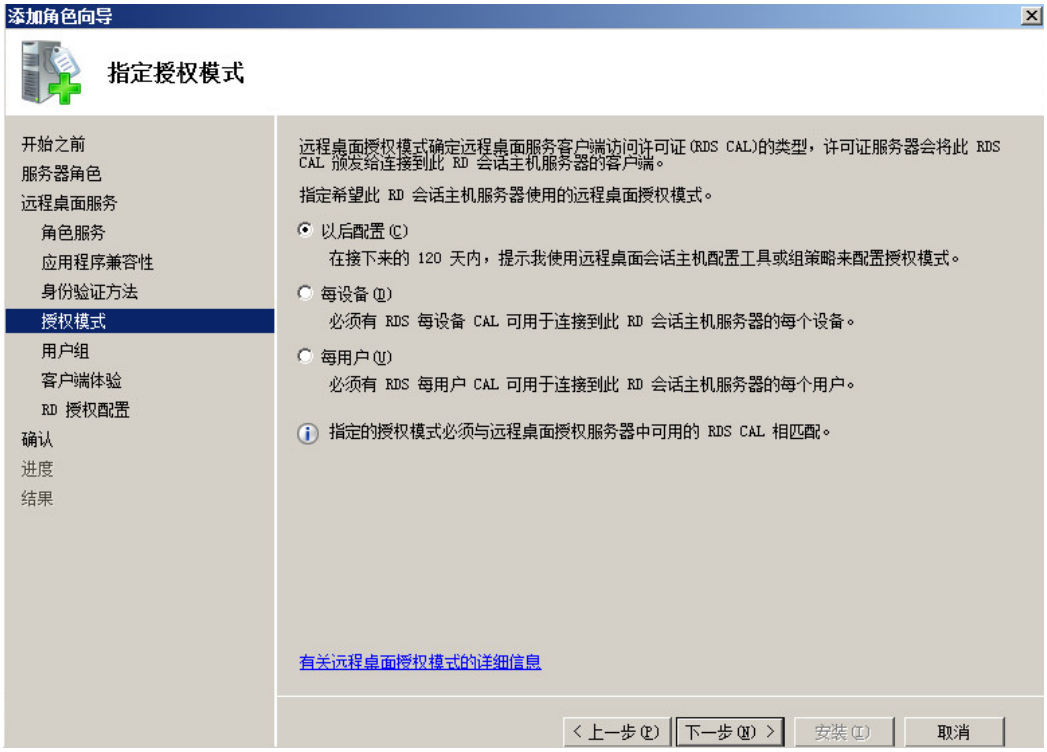
(7)　单击<下一步>进入身份验证方法窗口，选择“不需要使用网络级别身份验证”。

图8 选择身份验证方法示意图



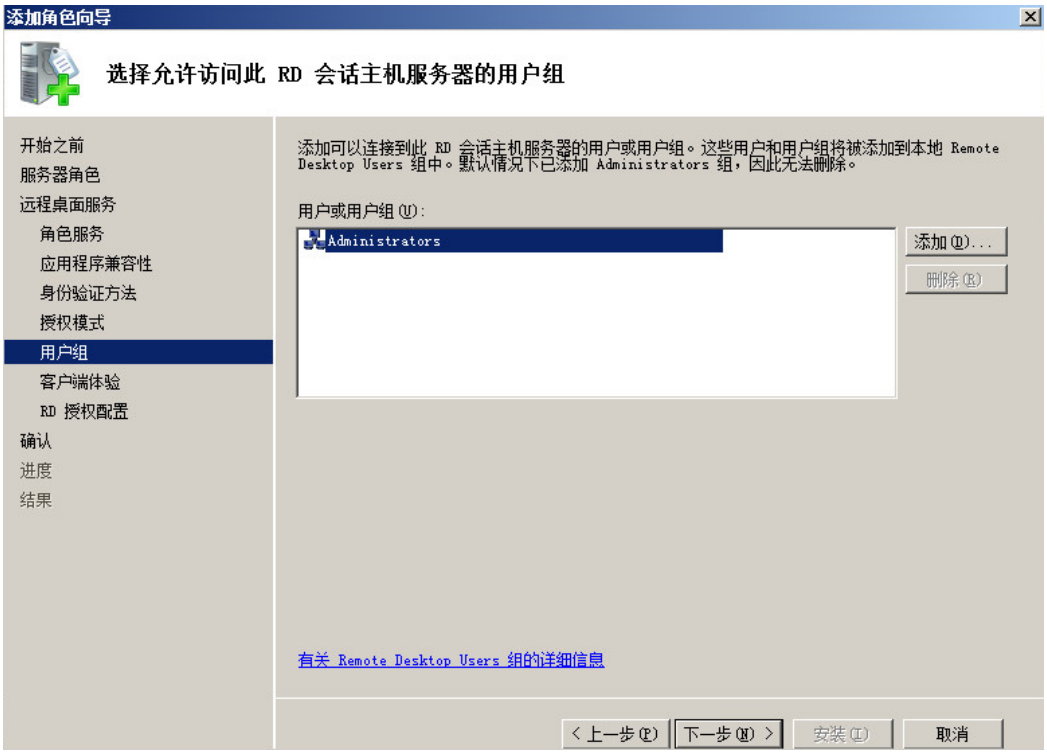
(8)　单击<下一步>进入授权模式窗口，选择“以后配置”。

图9 选择授权模式示意图



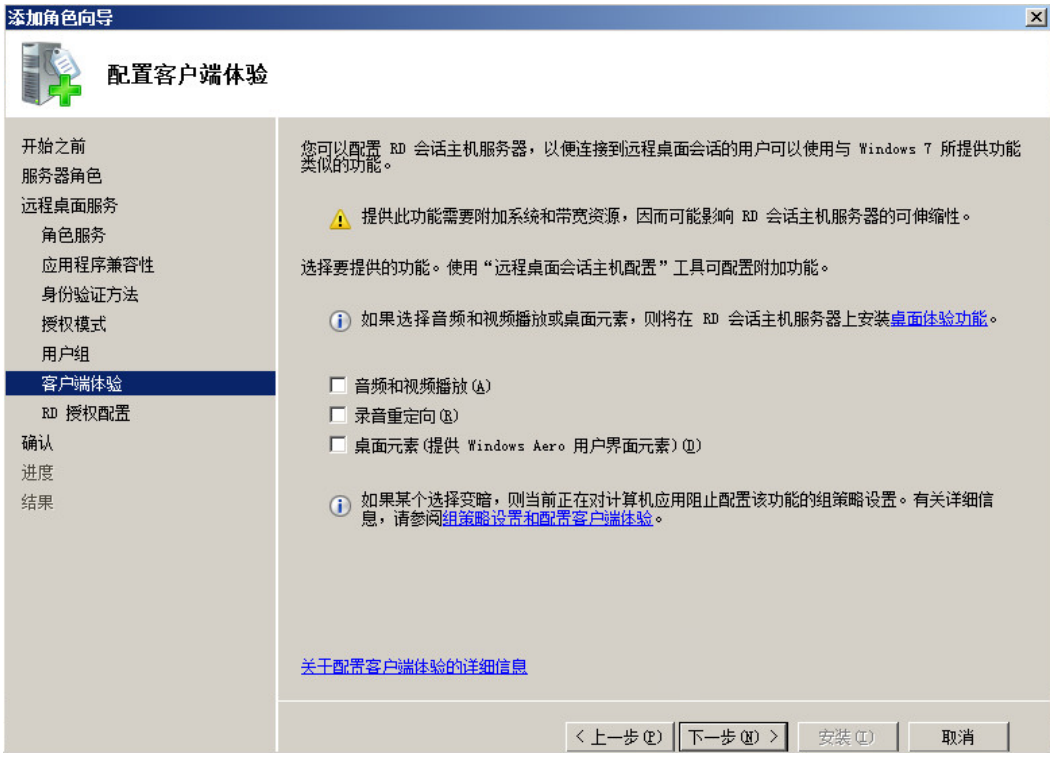
(9)　单击<下一步>进入用户组窗口，可在“用户或用户组”框添加允许远程访问的用户或用户组。

图10 添加用户组示意图



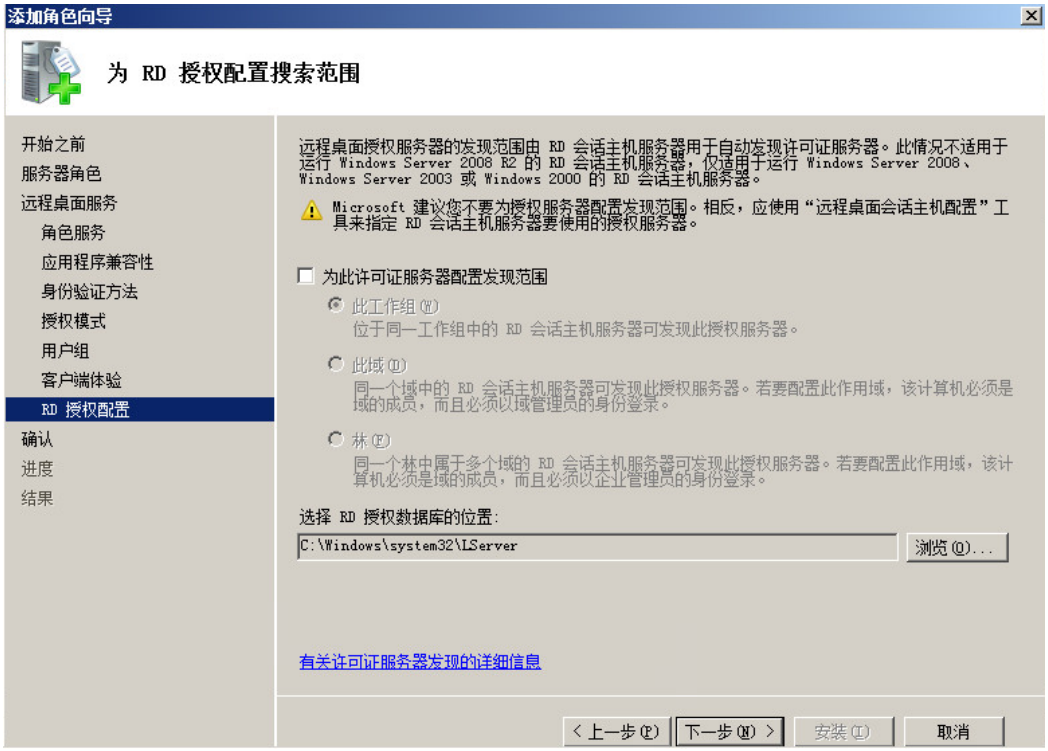
(10) 单击<下一步>进入客户端体验窗口，不选择任何功能项。

图11 选择客户端体验示意图



(11) 单击<下一步>进入 RD 授权配置窗口，不选择任何功能项。

图12 RD 授权配置界面示意图

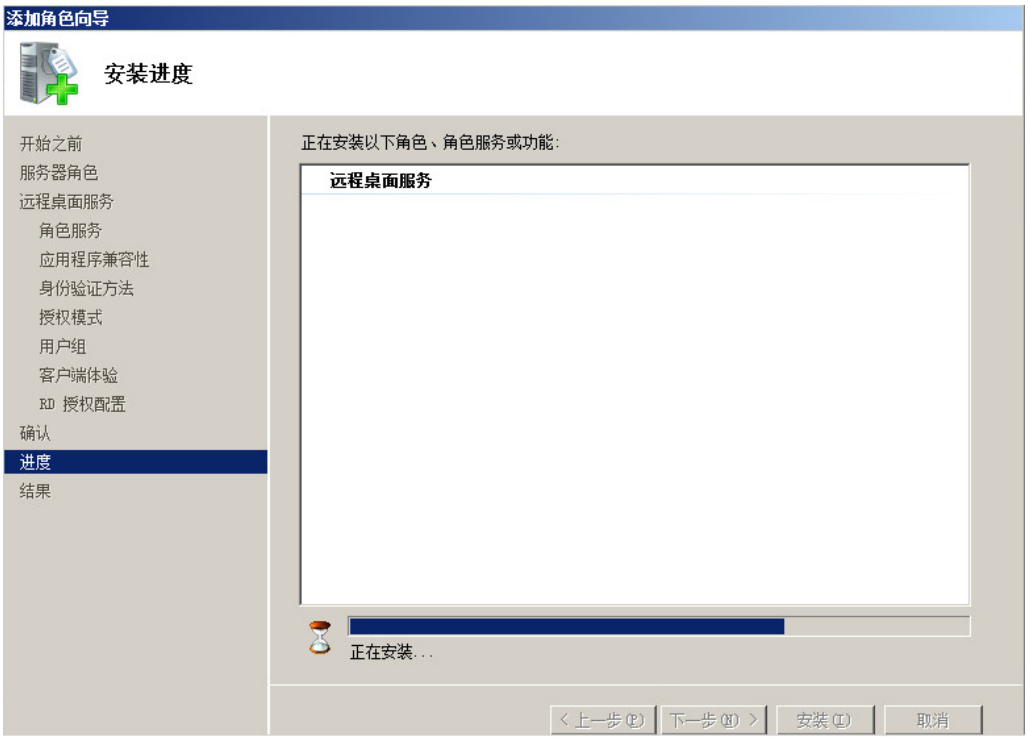


(12) 单击<下一步>进入确认窗口

图13 确认安装选择示意图

(13) 单击<安装>进入安装进度窗口。

图14 安装进度示意图

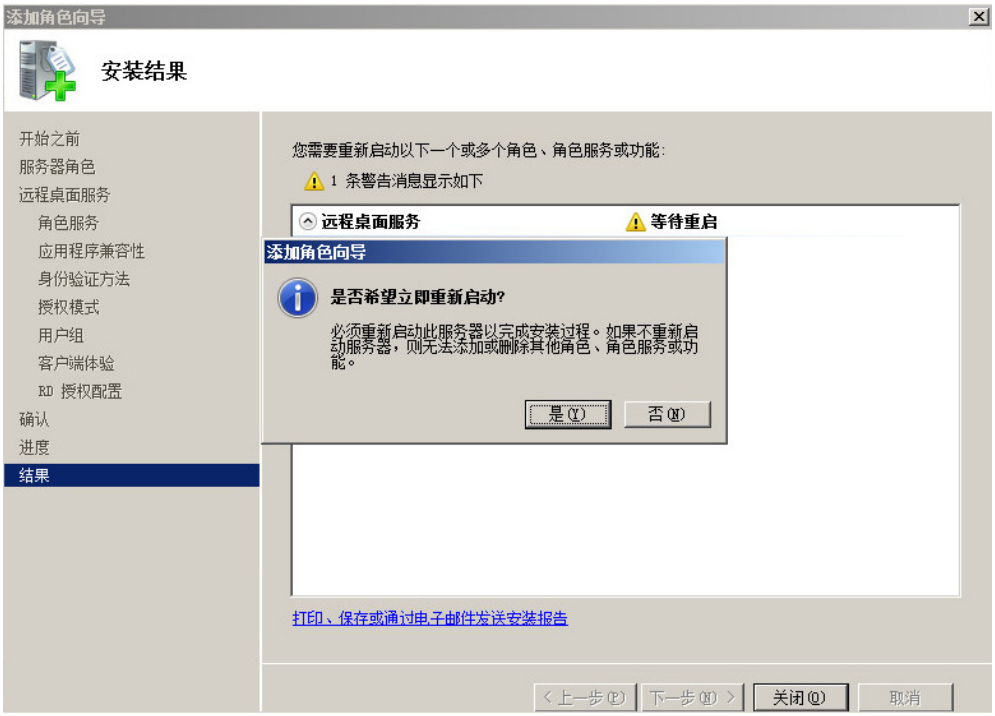


(14) 等待安装进度完成后，自动进入安装结果窗口，并提示需要重启服务器才能完成安装过程。

图15 安装结果示意图

(15) 单击<关闭>后自动提示“是否希望立即重新启动”。

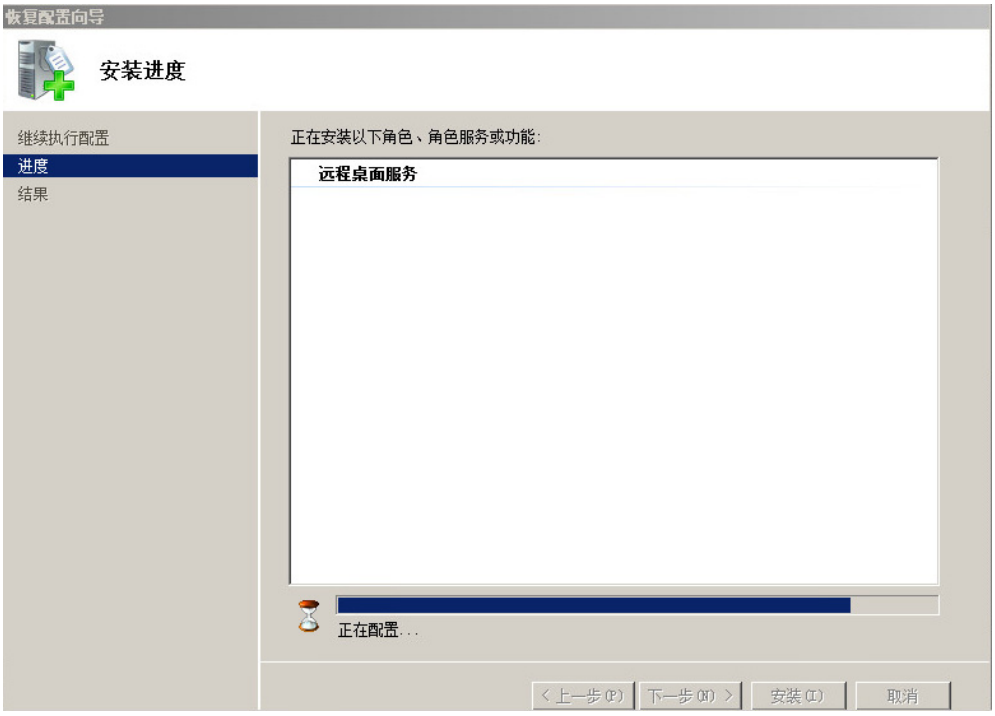
图16 是否需要重启提示示意图



(16) 单击<是>后，系统自动重新启动。

(17) 登录系统后，系统自动继续执行配置进度。

图17 安装进度示意图



(18) 自动完成安装结果，单击<关闭>即可。

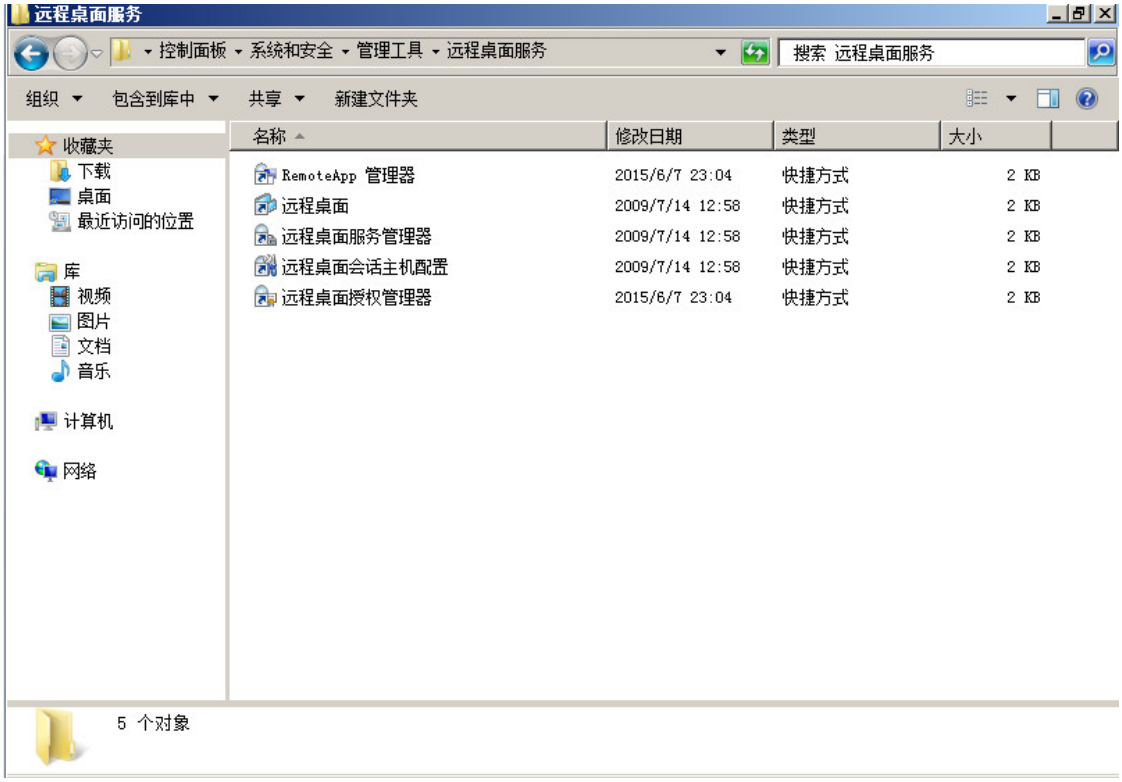
图18 安装成功提示示意图

3.2 应用中心激活授权（如果是测试客户，可忽略此操作）

3.2.1 激活应用中心

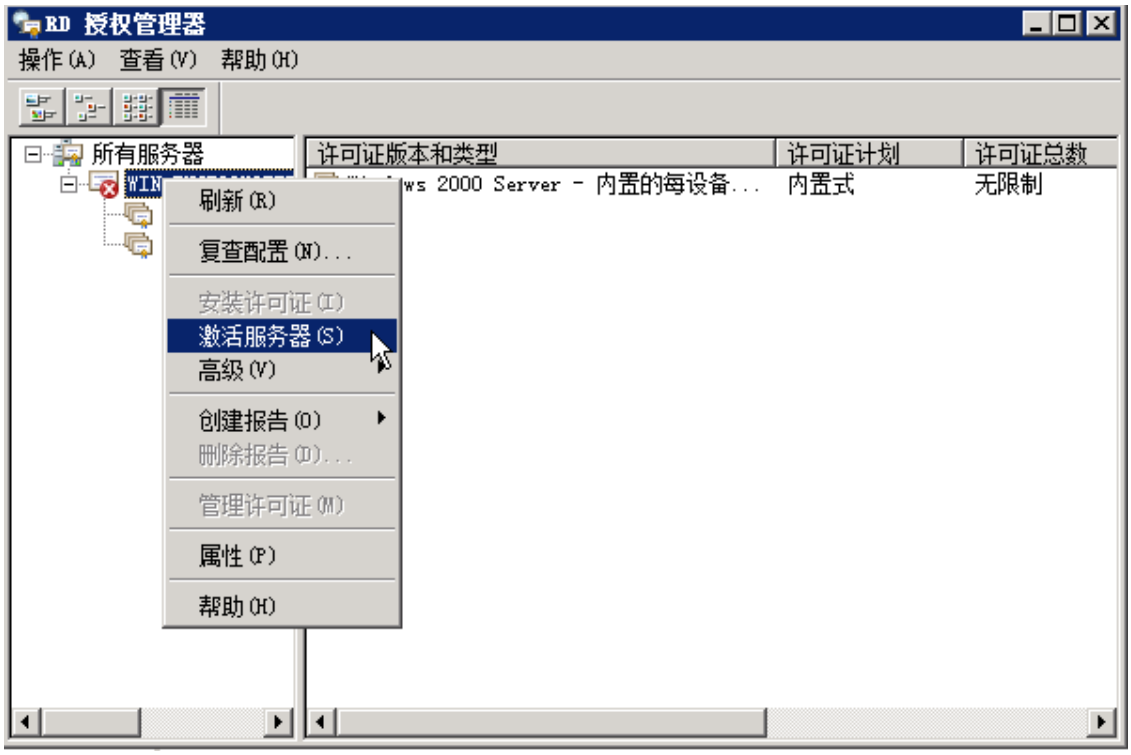
(1) 进入[控制面板/系统和安全/管理工具/远程桌面服务]界面中。

图19 远程桌面服务管理界面示意图



(2) 双击<远程桌面授权管理器>进入 RD 授权管理器界面，右击计算机名称。

图20 RD 授权管理器示意图



(3) 单击<激活服务器>进入服务器激活向导界面。

图21 服务器激活向导示意图

(4) 单击<下一步>进入连接方法界面，本手册以“Web 浏览器”的连接方法为例。

图22 选择连接方法示意图

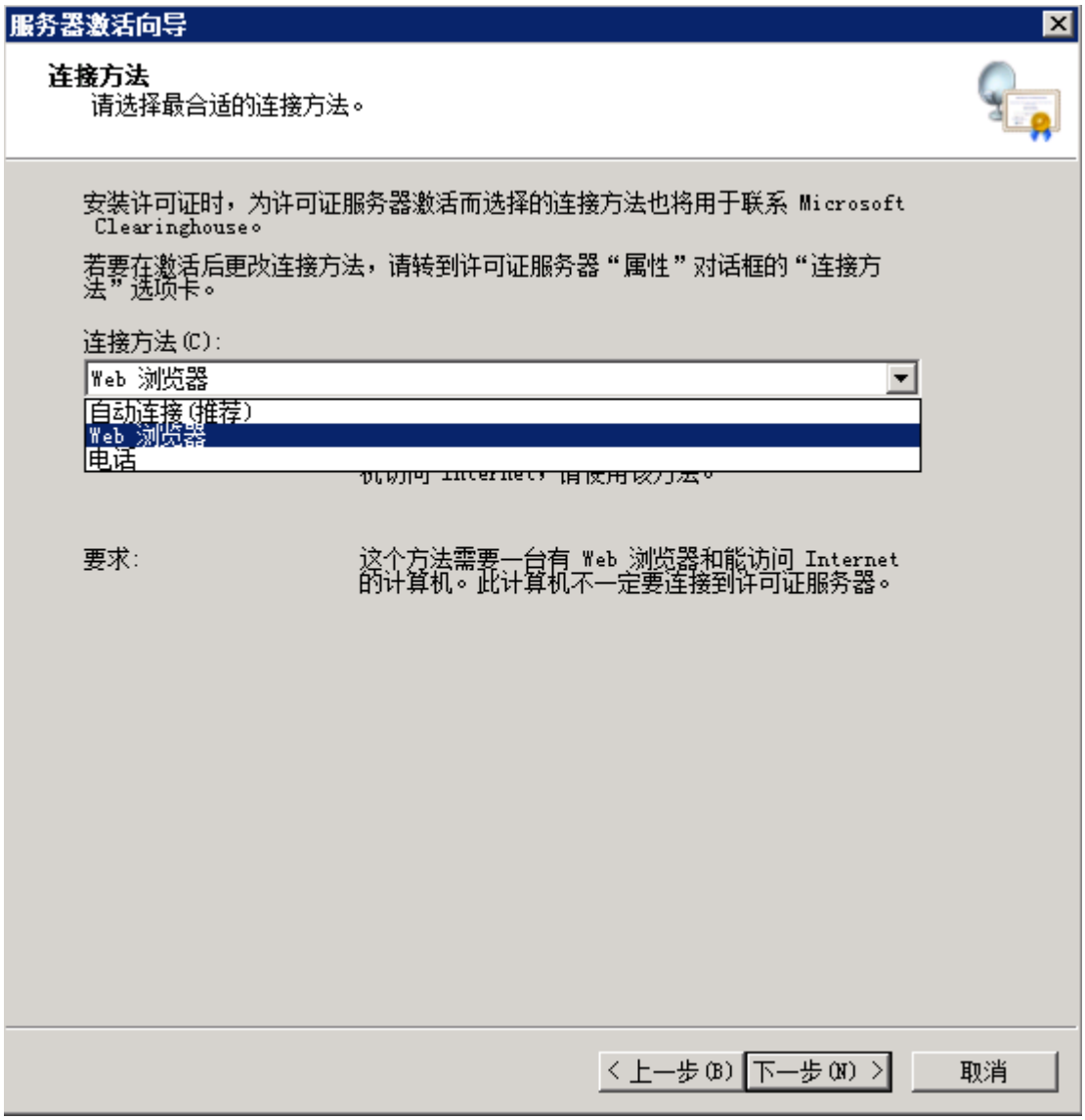


表2 连接方法说明

连接方法	描述
自动连接（推荐）	使用此方法的前提是要确保应用中心能连通互联网，否则无法进行授权许可。
Web浏览器	此方法适用于应用中心无法连通互联网，但需要进行授权许可。 找一台能连通互联网的windows电脑，在浏览器中输入https://activate.microsoft.com ，进入远程桌面服务器授权页面进行授权许可。
电话	此方法适用于通过微软的服务热线进行电话授权许可，此方法比较繁琐，需要提供各种详细信息。

(5) 单击<下一步>进入许可证服务器激活界面。

图23 许可证服务器激活示意图

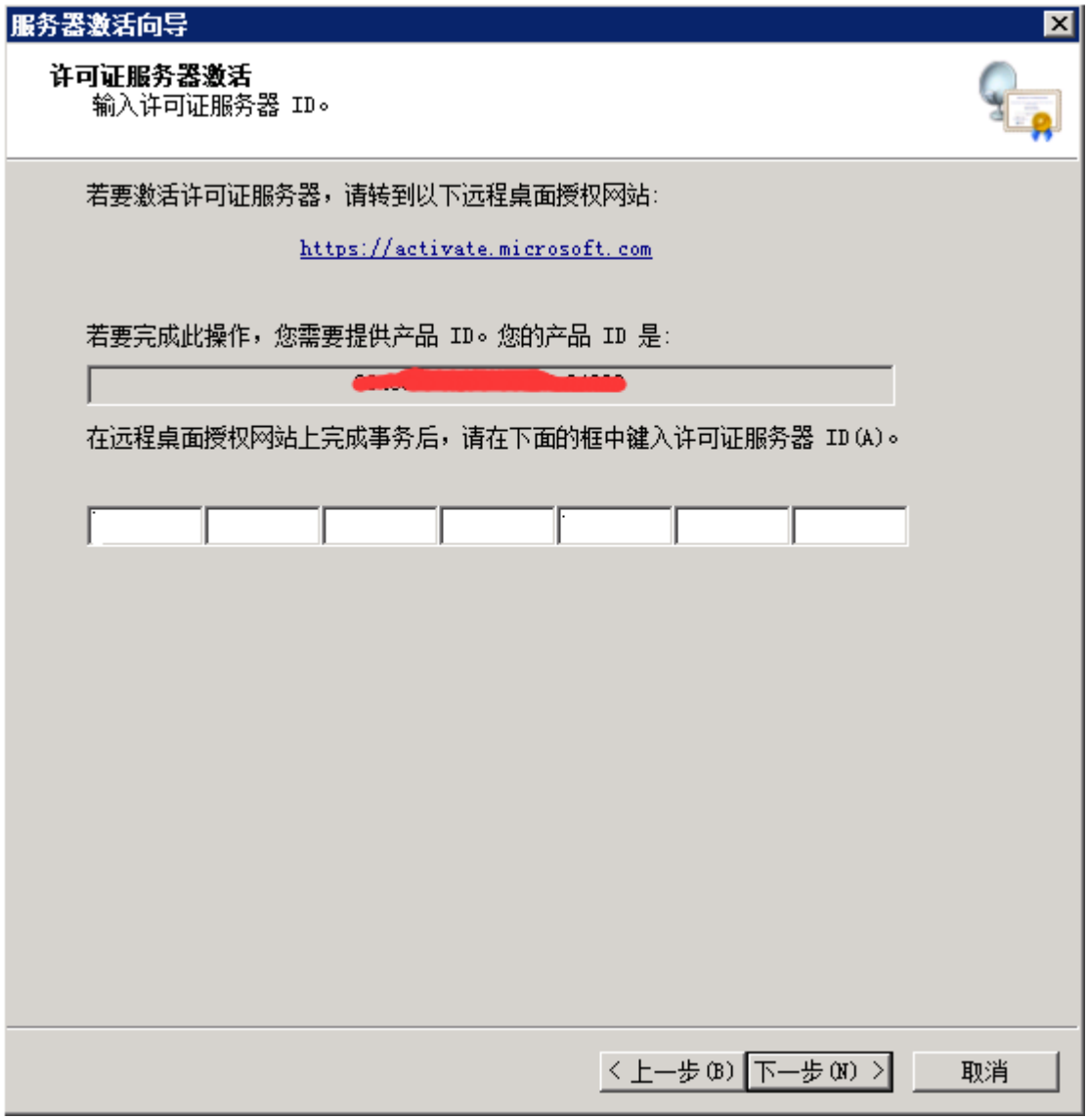
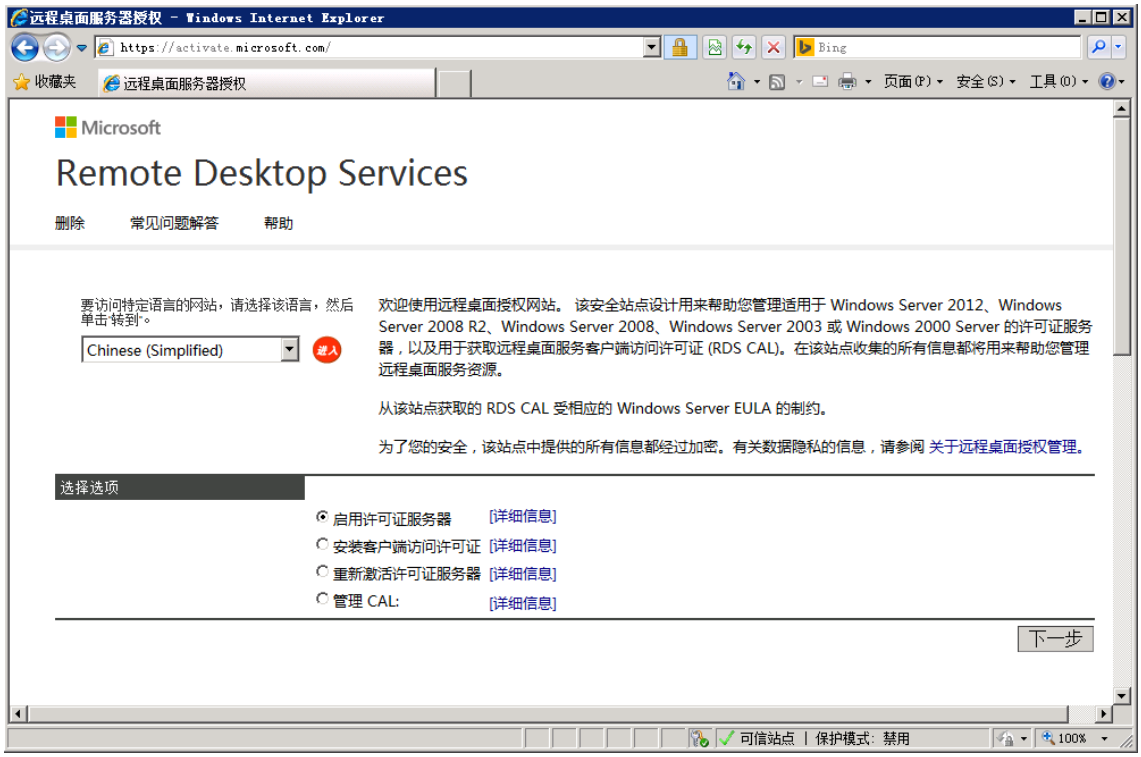


表3 服务器激活条件说明

激活条件	描述
远程桌面授权网站	• https://activate.microsoft.com
产品ID	• 操作系统的产品 ID，服务器激活向导界面会自动识别本操作系统的产品 ID。
许可证服务器ID	• 许可证服务器 ID 是由产品 ID 生成的，有了许可证服务器 ID 才能许可证服务器激活成功。

(6) 使用一台可以连通互联网的电脑，在浏览器中输入 https://activate.microsoft.com 进入 RDS 授权页面，选择“启用许可证服务器”。

图24 RDS 授权页面示意图



(7) 单击<下一步>进入 RDS 信息填写页面，输入应用中心的产品 ID、公司名称、国家(地区)。

图25 RDS 授权页面示意图

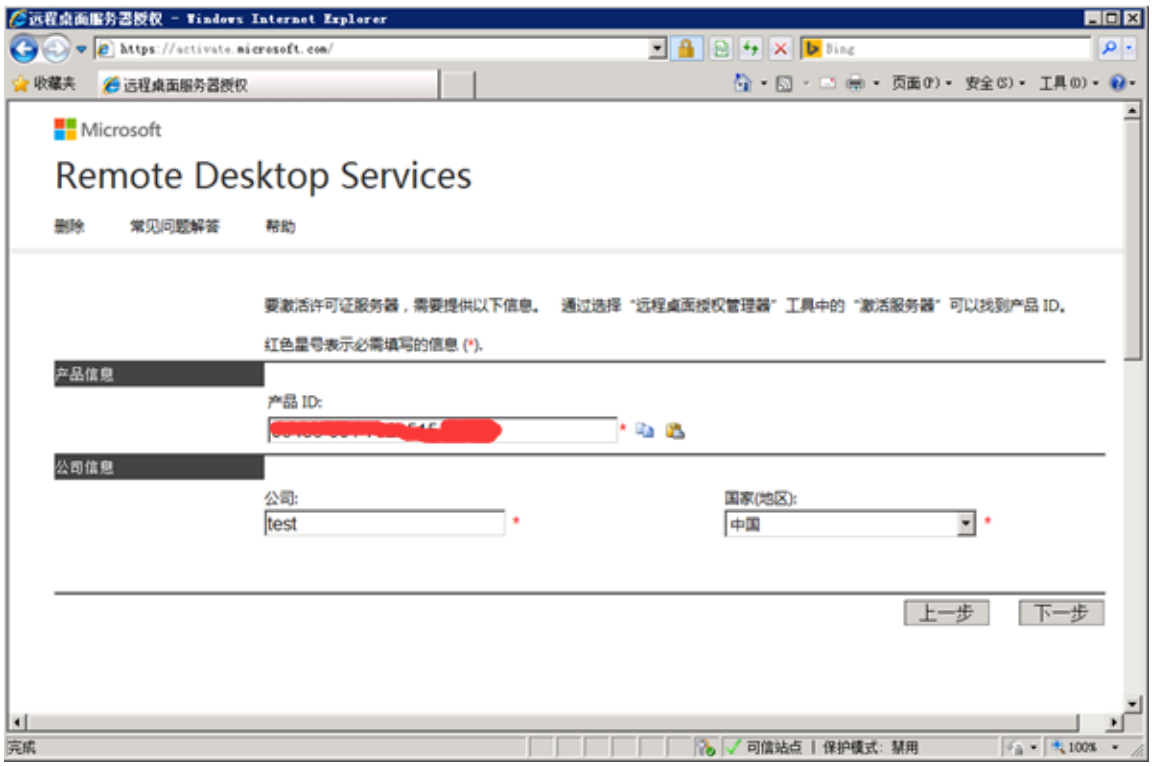
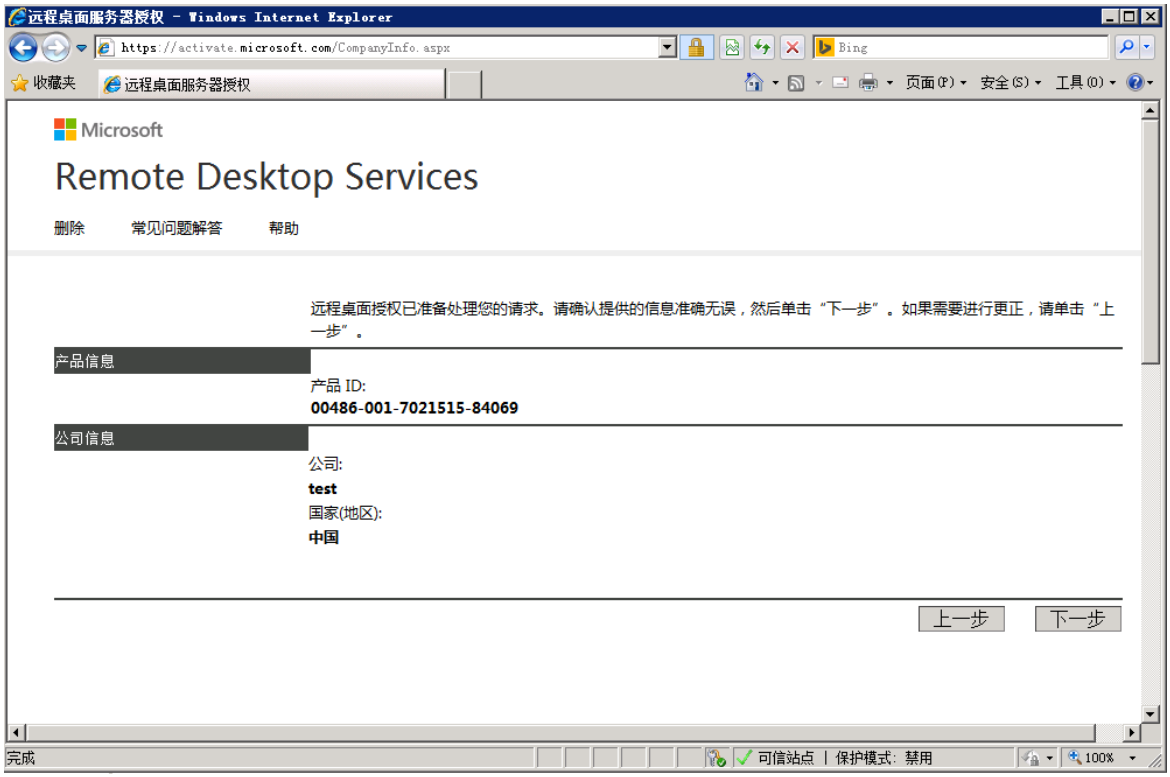


表4 RDS 授权信息说明

填写项	描述
产品ID	将服务器激活向导界面的产品ID填写进去 如需查看产品ID，请右击应用中心里的“计算机”，单击<属性>进入系统属性界面查看
公司	填写使用用户单位的名称
国家（地区）	选择应用中心所在国家或地区

(8) 单击<下一步>进入 RDS 授权信息确认页面。

图26 RDS 授权页面示意图

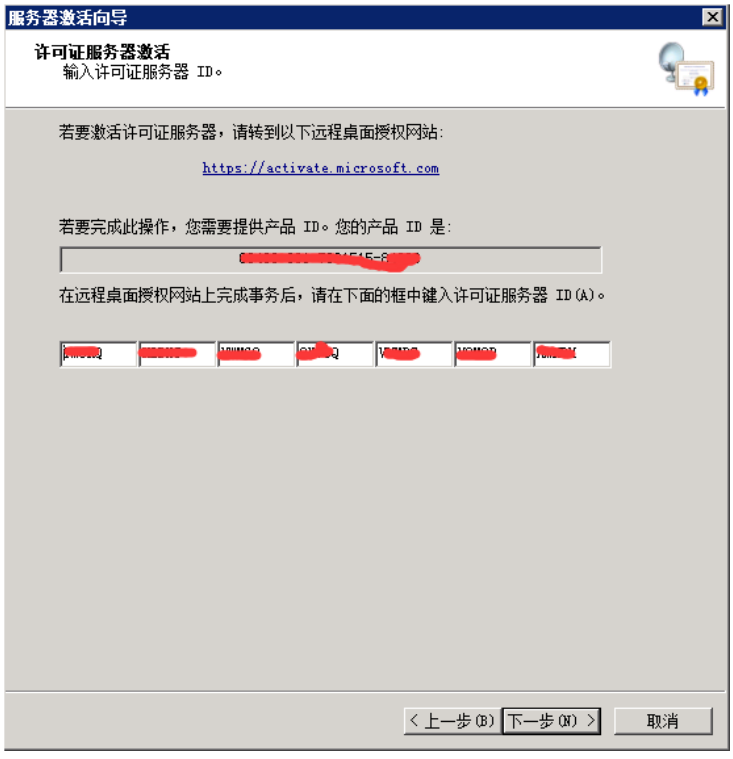


(9) 单击<下一步>RDS 授权一个许可证服务器 ID，将其复制并保存好。

图27 RDS 授权页面示意图

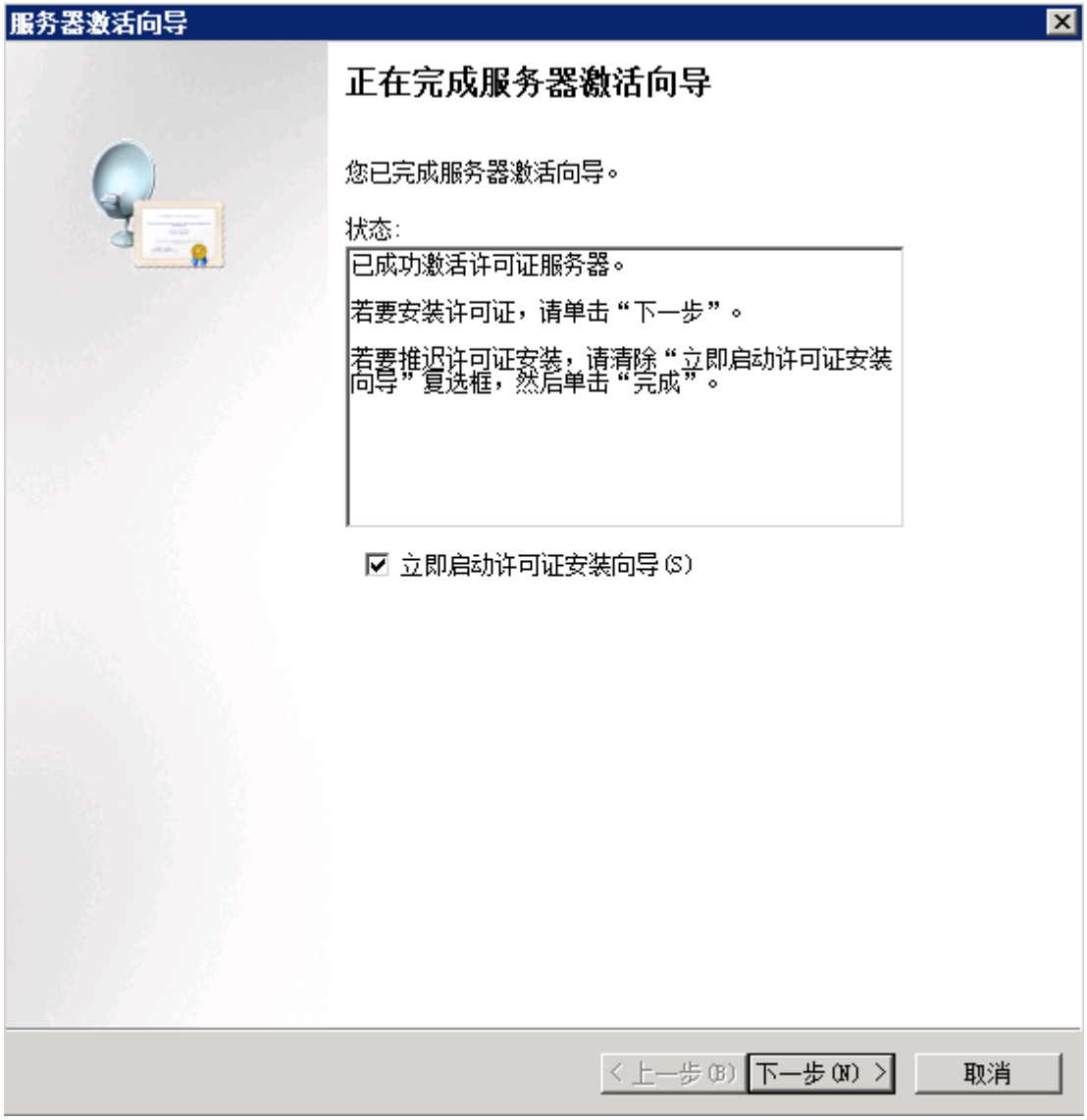
(10) 返回到应用中心里的[服务器激活向导]界面，输入 RDS 授权页面生成的许可证服务器 ID。

图28 许可证服务器激活示意图



(11) 单击<下一步>进入正在完成服务器激活向导界面。

图29 完成服务器激活向导示意图



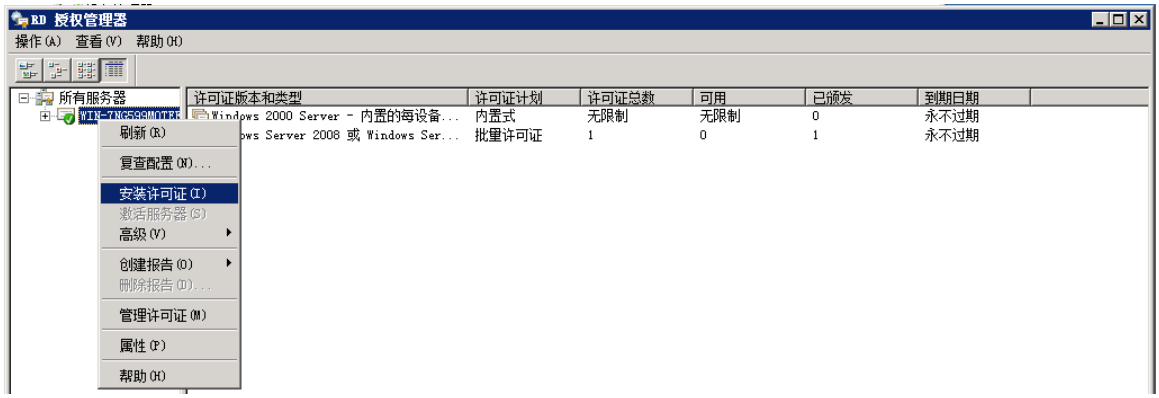
(12) 如果单击<下一步>则直接进入许可证安装向导界面，如 3.2.2 (2)图 31。

如果单击<取消>则直接退出服务器激活向导界面。

3.2.2 安装应用中心授权许可证

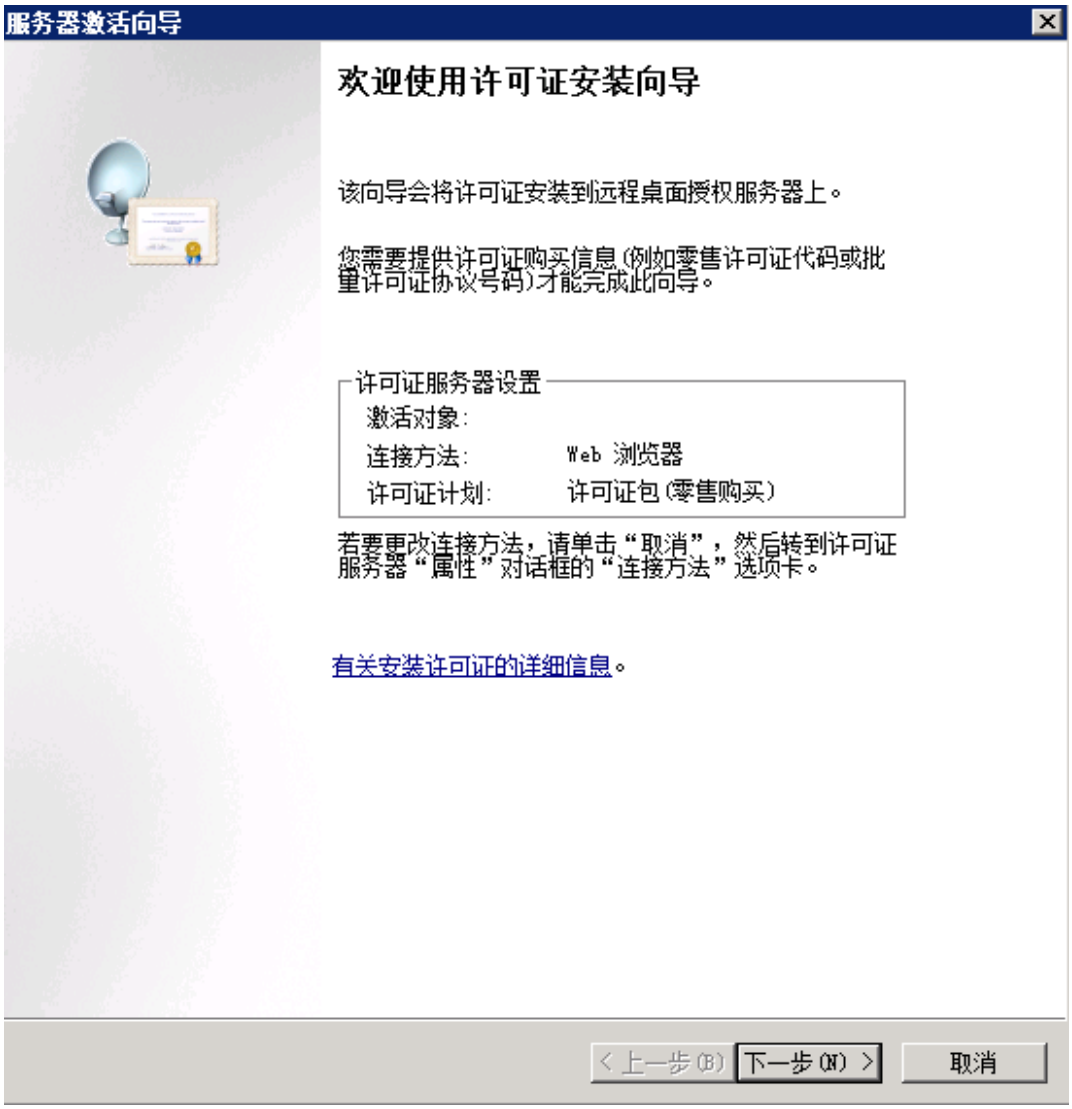
(1) 在[RD 授权管理器]中右击计算机名称。

图30 RD 授权管理器示意图



(2) 单击<安装许可证>进入许可证安装向导界面。

图31 许可证安装向导示意图



(3) 单击<下一步>进入获取客户端许可证密钥包界面。

图32 获取客户端许可证密钥包界面示意图

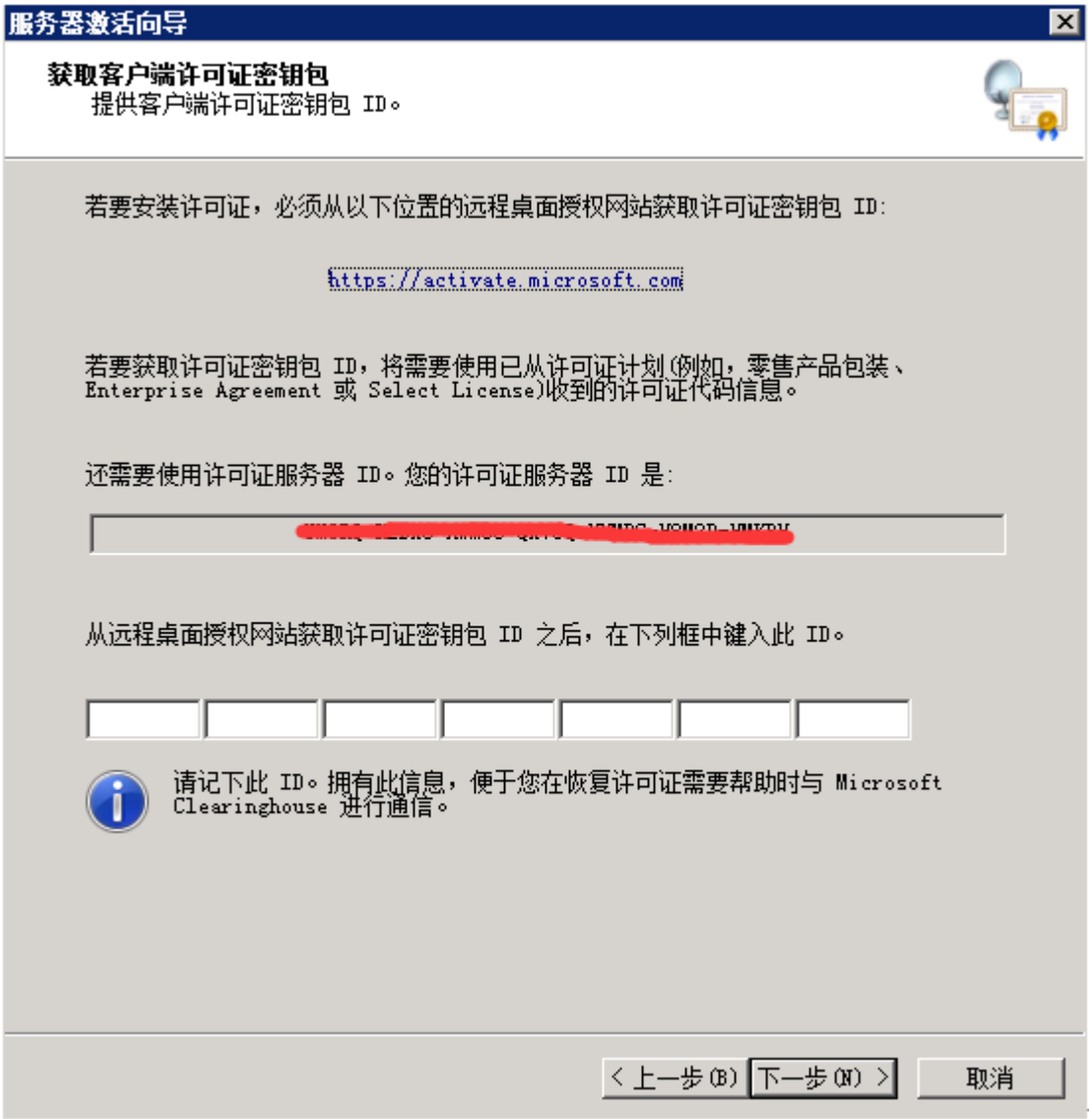


表5 获取客户端许可证密钥包条件说明

获取条件	描述
远程桌面授权网站	https://activate.microsoft.com
许可证服务器ID	许可证安装向导界面会自动识别本操作系统的许可证服务器ID。
许可证密钥包ID	许可证密钥包ID是由许可证服务器ID、父级计划和开放式许可证详细信息的号码共同生成的。 在(6)中会用到应用中心授权许可证中的父级计划和开放式许可证详细信息的号码。

(4) 使用一台可以连通互联网的电脑，在浏览器中输入 https://activate.microsoft.com 进入 RDS 授权页面，选择“安装客户端访问许可证”。

图33 RDS 授权页面示意图

(5) 单击<下一步>进入 RDS 授权信息填写页面，输入正确的许可证服务器 ID，在许可证程序里选择“开放式许可证”，填写公司名称，选择正确的国家(地区)。

图34 RDS 授权页面示意图

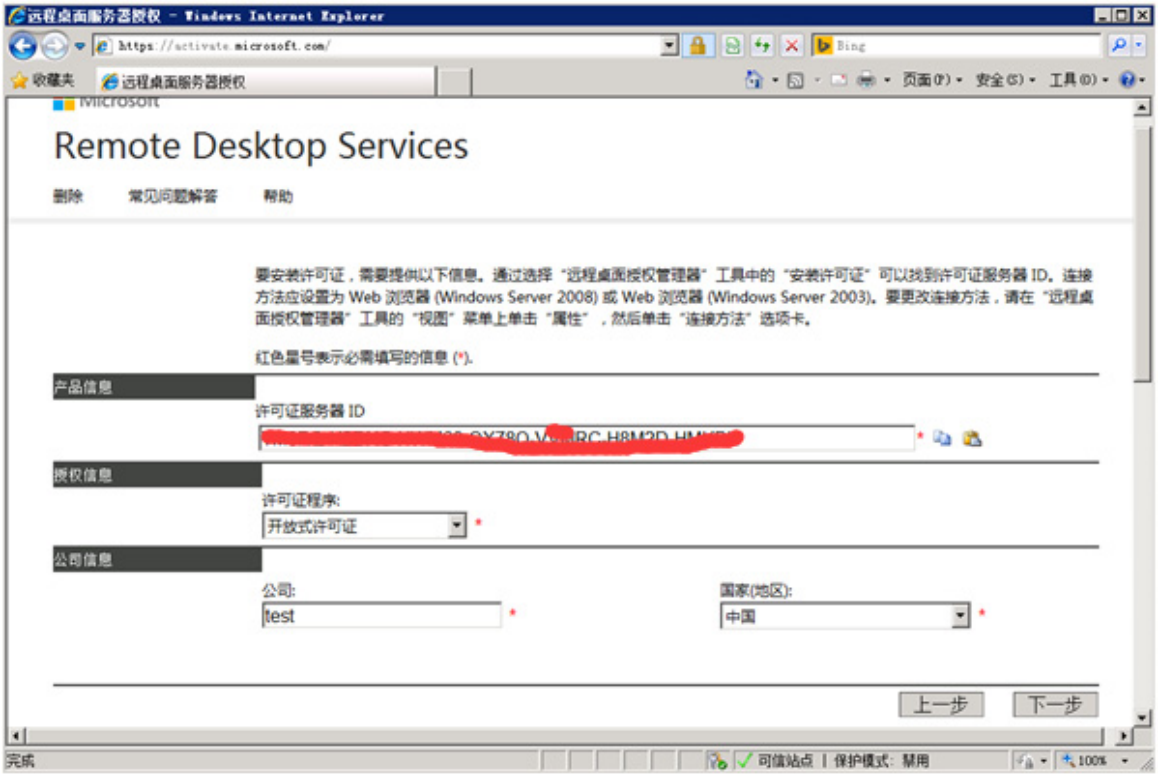


表6 RDS 授权信息说明

填写项	描述
许可证服务器ID	将获取客户端许可证密钥包界面的许可证服务器ID填写进去。
许可证程序	选择“开放式许可证”。
公司	填写使用用户单位的名称。
国家(地区)	选择应用中心所在国家或地区。

(6) 单击<下一步>进入 RDS 授权许可证信息填写页面，选择“windows server 2008 R2 每设备 CAL 或 windwos server 2008 TS 每设备 CAL”，填写正确的 RDS 授权数量、授权号码、许可证号码。

图35 RDS 授权页面示意图

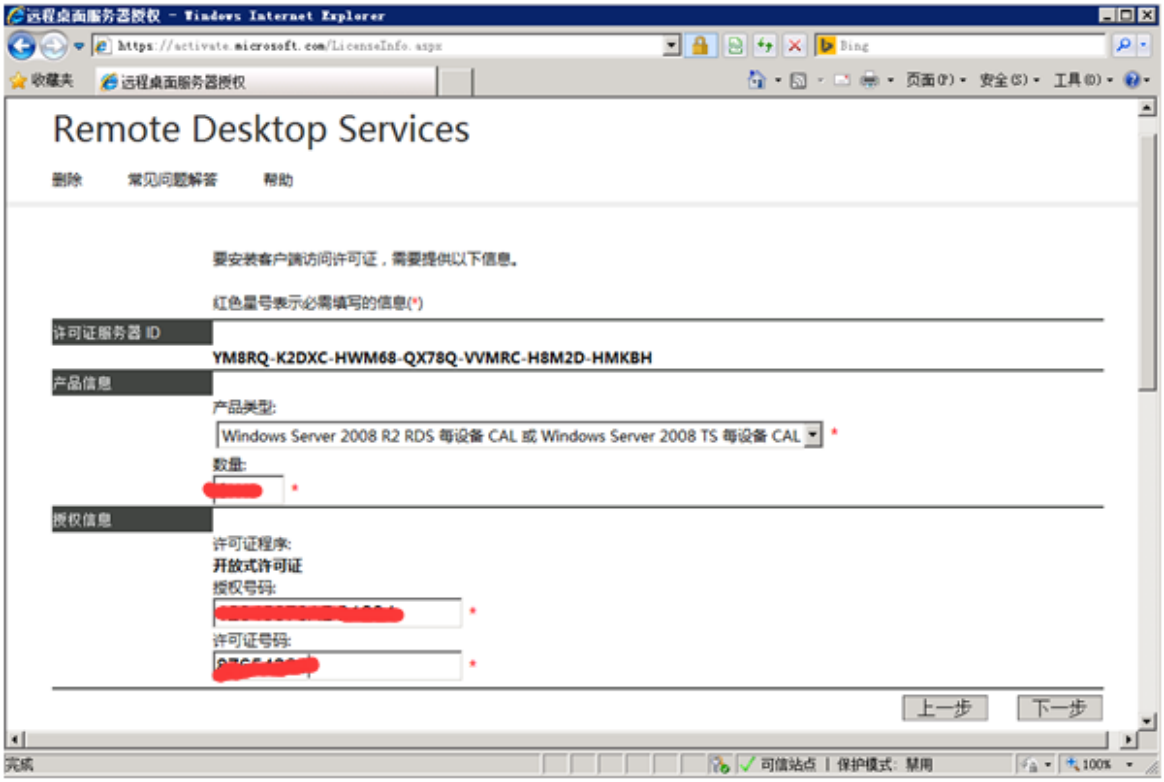


表7 RDS 授权信息说明

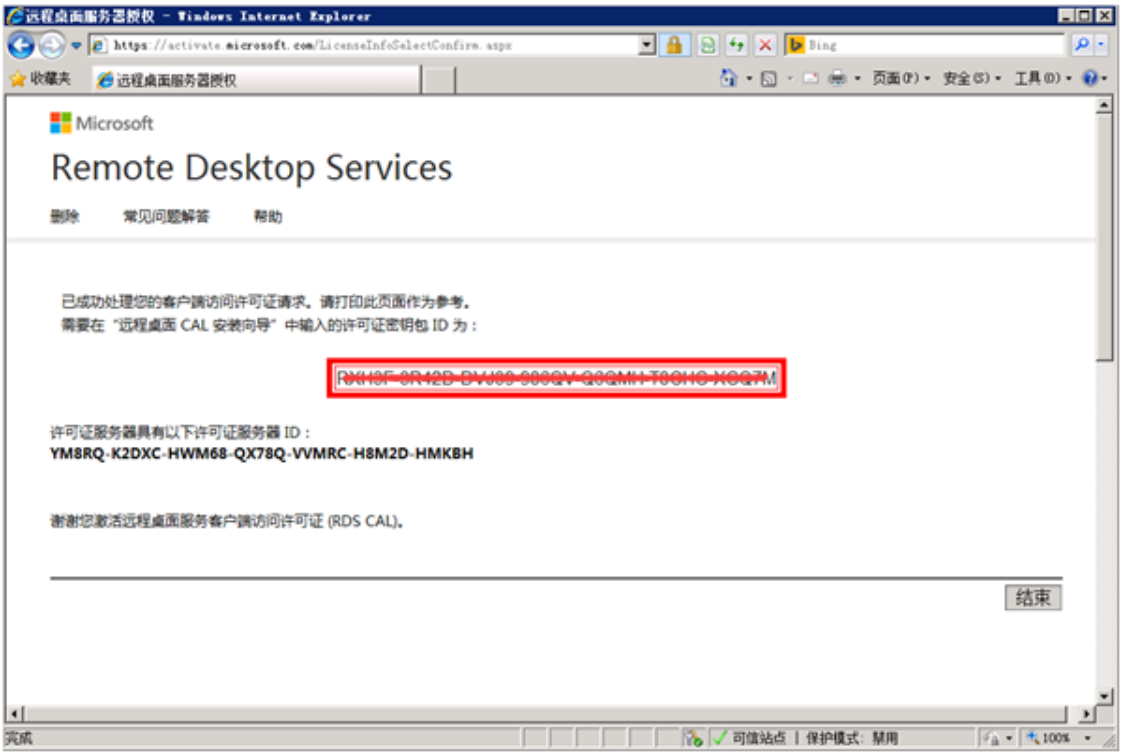
填写项	描述
许可证服务器ID	将获取客户端许可证密钥包界面的许可证服务器ID，此处不需要填写。
产品类型	请选择“windows server 2008 R2每设备CAL或windwos server 2008 TS每设备CAL”的RD授权模式。
数量	填写RDS对应的数量，数量自定义，可以根据堡垒机的资产数量填写数量。
许可证程序	开放式许可证
授权号码	根据应用中心授权许可证中提供的“父级计划”号码填写。
许可证号码	根据应用中心授权许可证中提供的“开放式许可证详细信息”号码填写。

(7) 单击<下一步>进入 RDS 授权信息确认页面。

图36 RDS 授权页面示意图

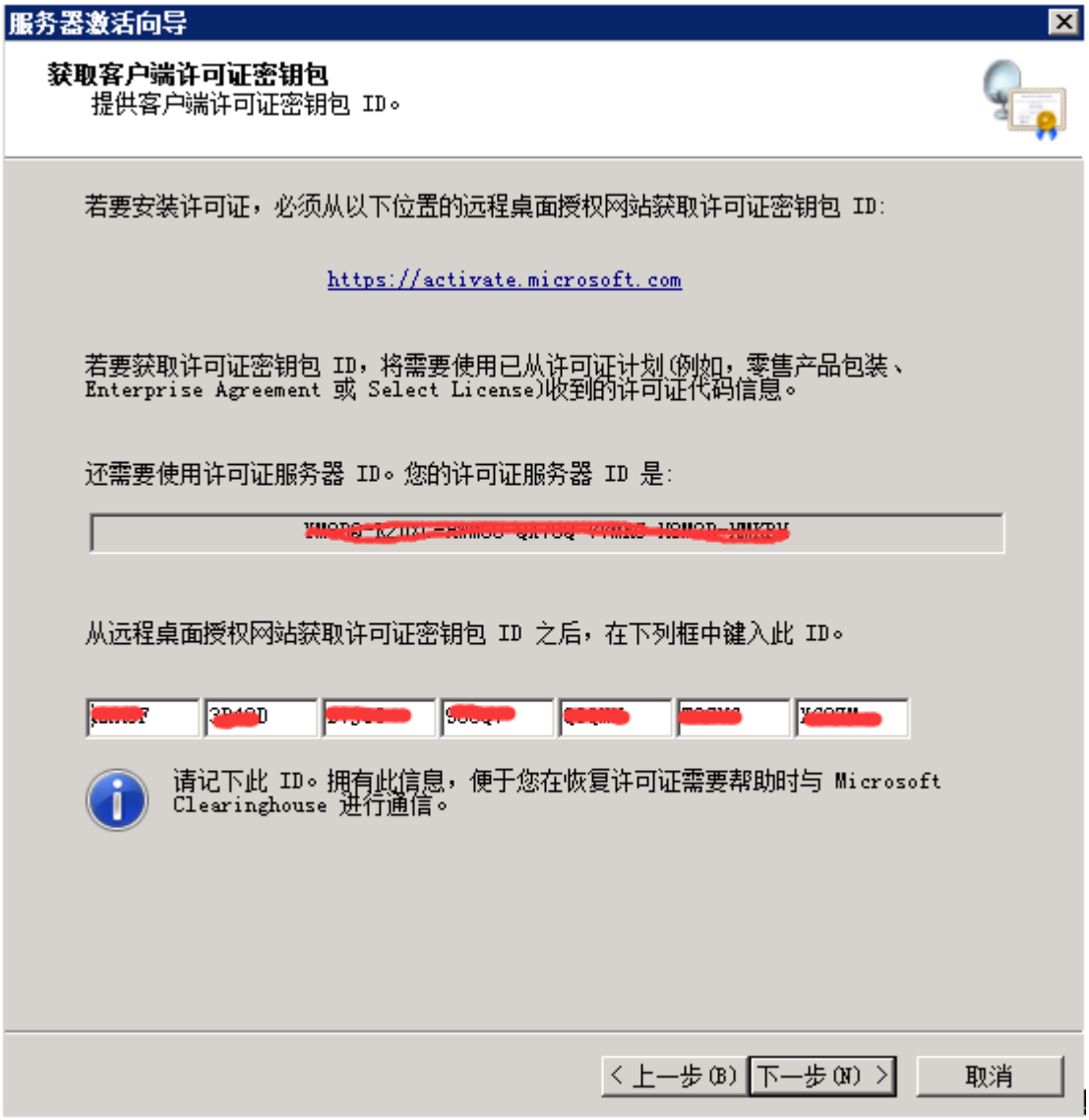
(8) 单击<下一步>RDS 授权一个许可证密钥包 ID 号，将其复制并保存好。

图37 RDS 授权页面示意图



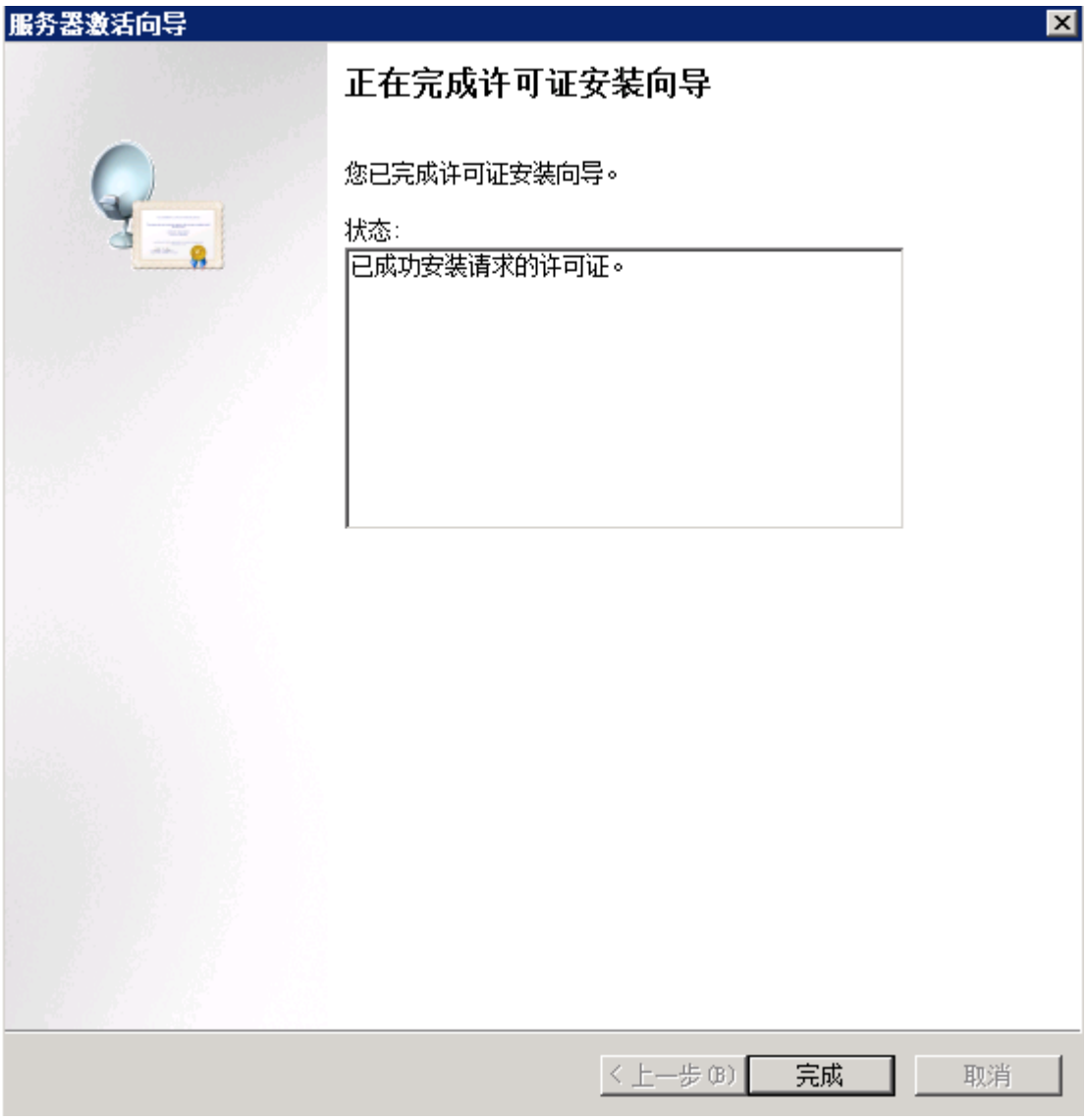
(9)　返回至获取客户端许可证密钥包界面，输入 RDS 授权页面生成的许可证密钥包 ID。

图38 服务器激活向导示意图



(10) 单击<下一步>进入正常完成许可证安装向导界面。

图39 完成许可证安装向导示意图



(11) 单击<完成>后即可在 RD 授权管理器界面中看到已成功授权，并且已经变成绿色的勾勾。

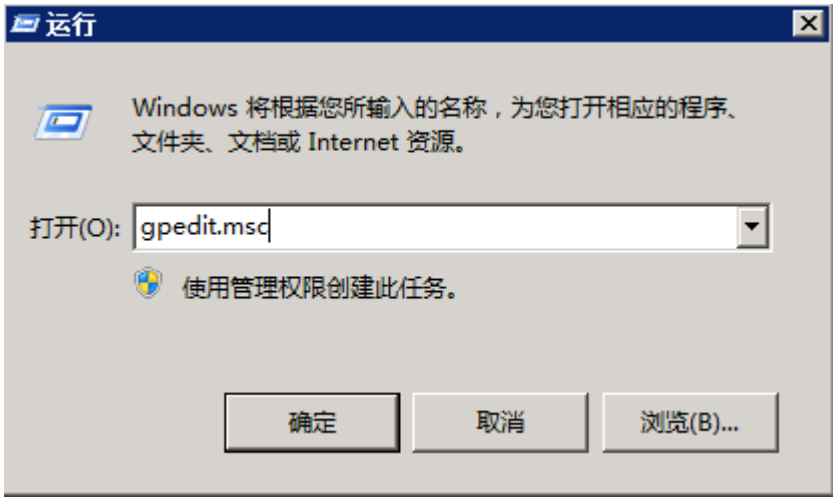
图40 RD 授权管理器示意图

3.3 调整应用中心的策略（必配步骤）

3.3.1 调整本地组策略

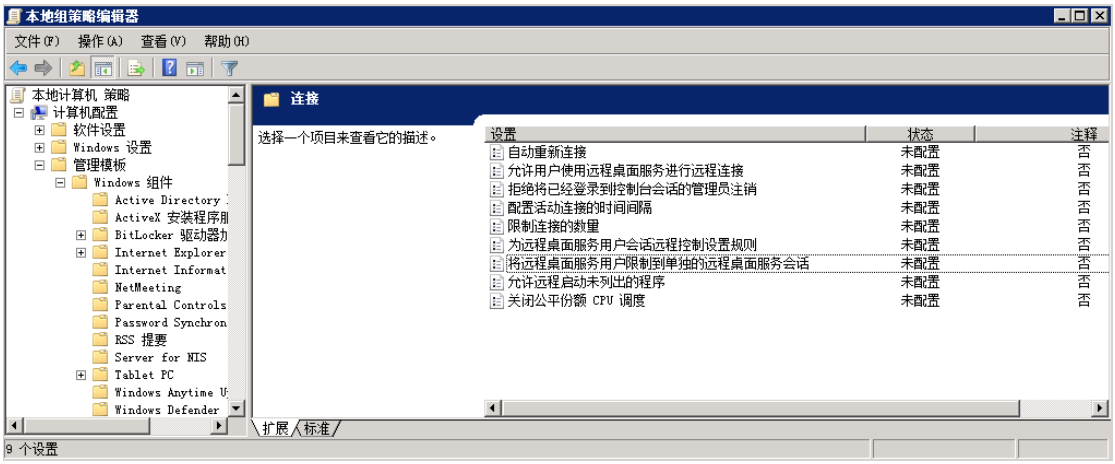
(1) 在运行窗口中输入“gpedit.msc”。

图41 运行窗口示意图



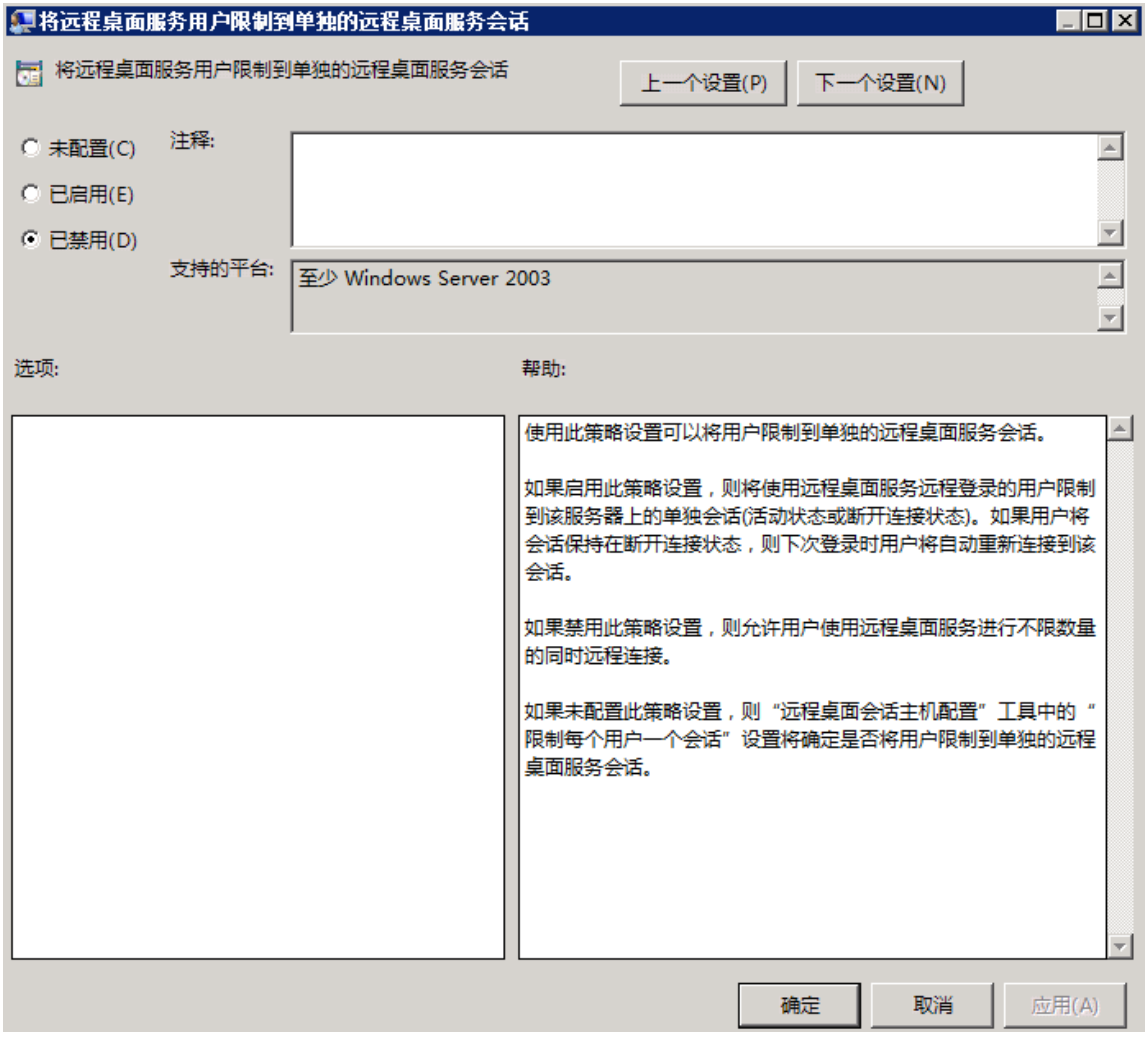
(2) 单击<确定>进入[计算机配置/管理模板/windows 组件/远程桌面服务/远程桌面会话主机/连接]界面。

图42 本地组策略示意图



(3) 双击<将远程桌面服务用户限制到单独的远程桌面服务会话>，在配置界面中选择“已禁用”。

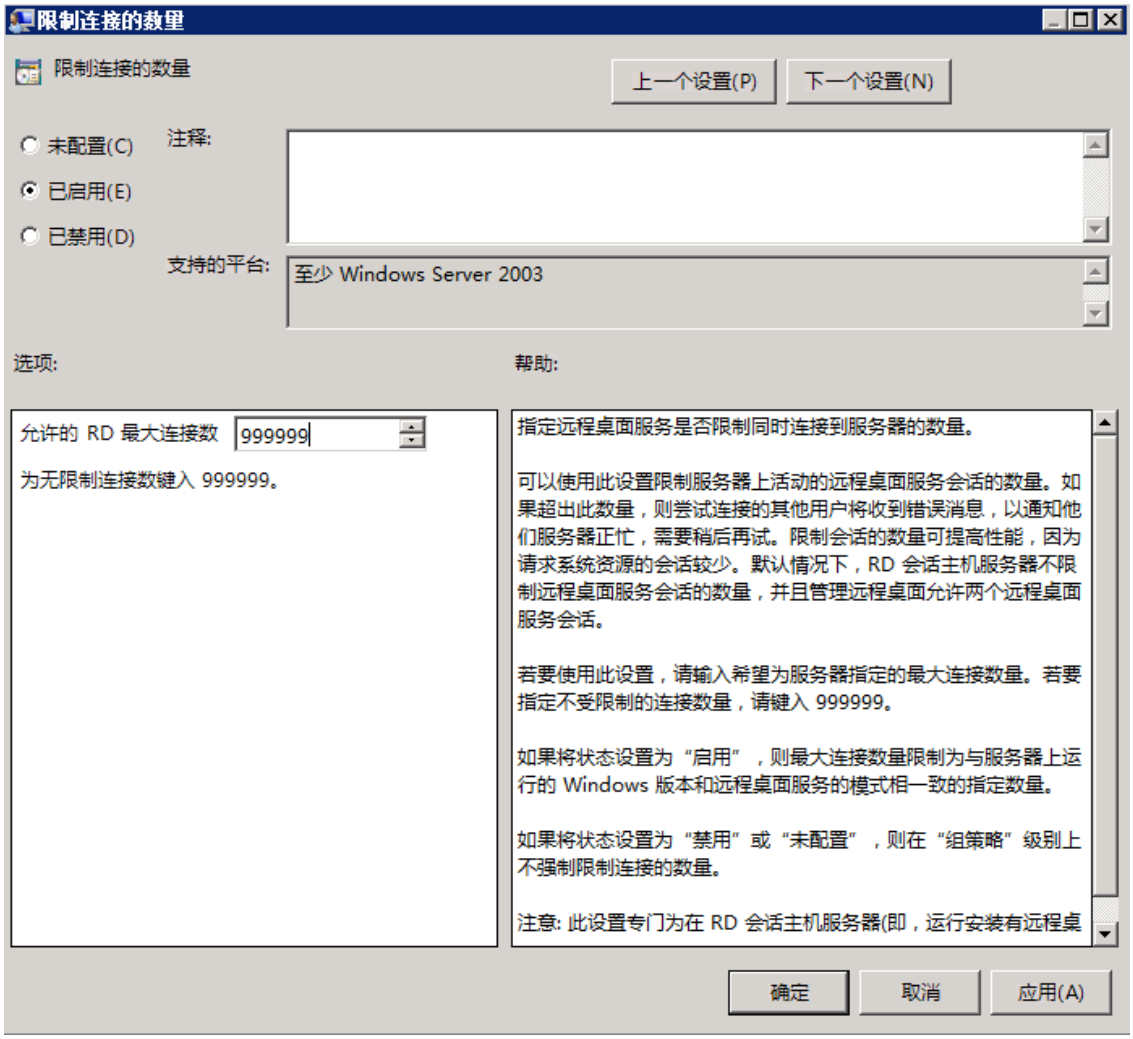
图43 策略配置示意图



单击<确定>即可。

(4) 双击<限制连接的数量>，在配置界面中选择“已启用”，并设置允许的 RD 最大连接数为“999999”。

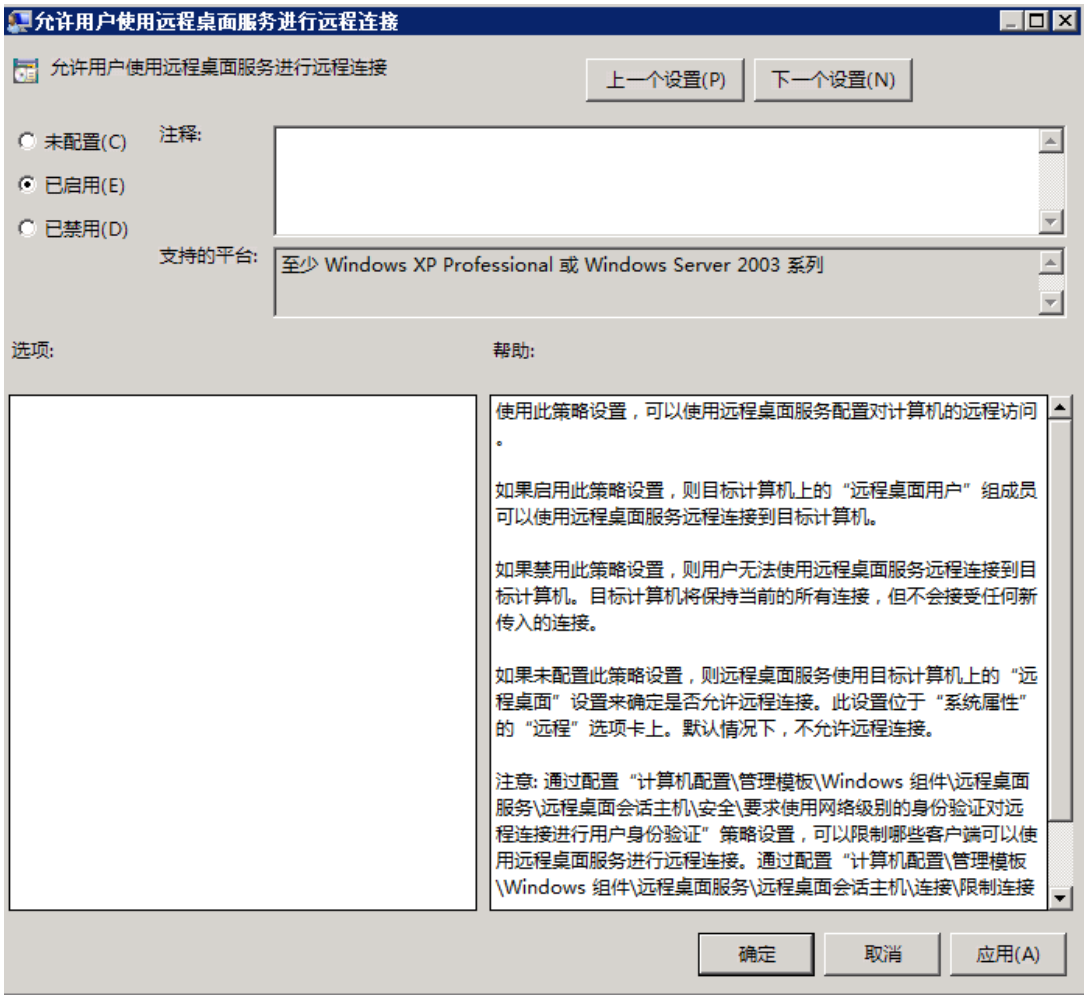
图44 策略配置示意图



单击<确定>即可。

(5) 双击<允许用户使用远程桌面服务进行远程连接>，在配置界面中选择“已启用”。

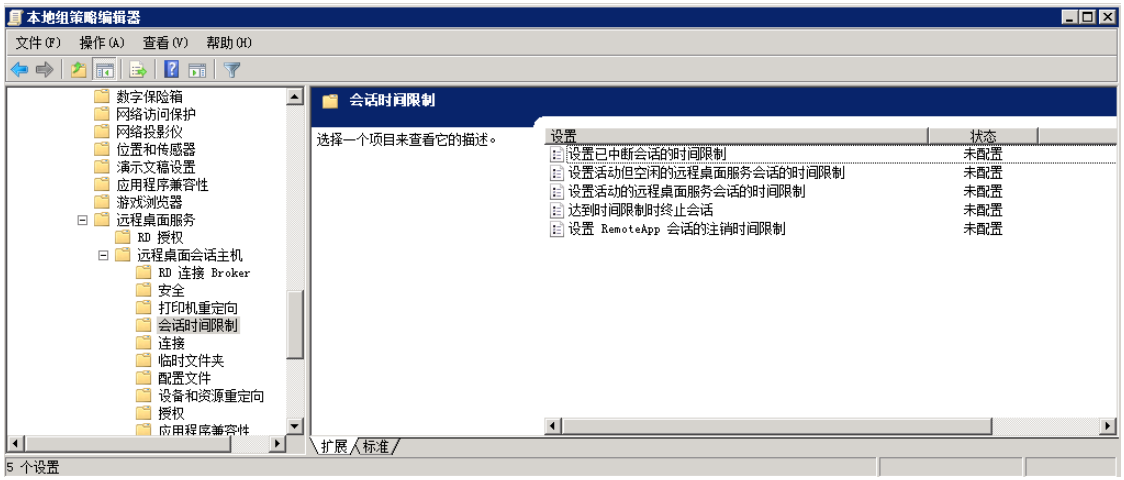
图45 策略配置示意图



单击<确定>即可。

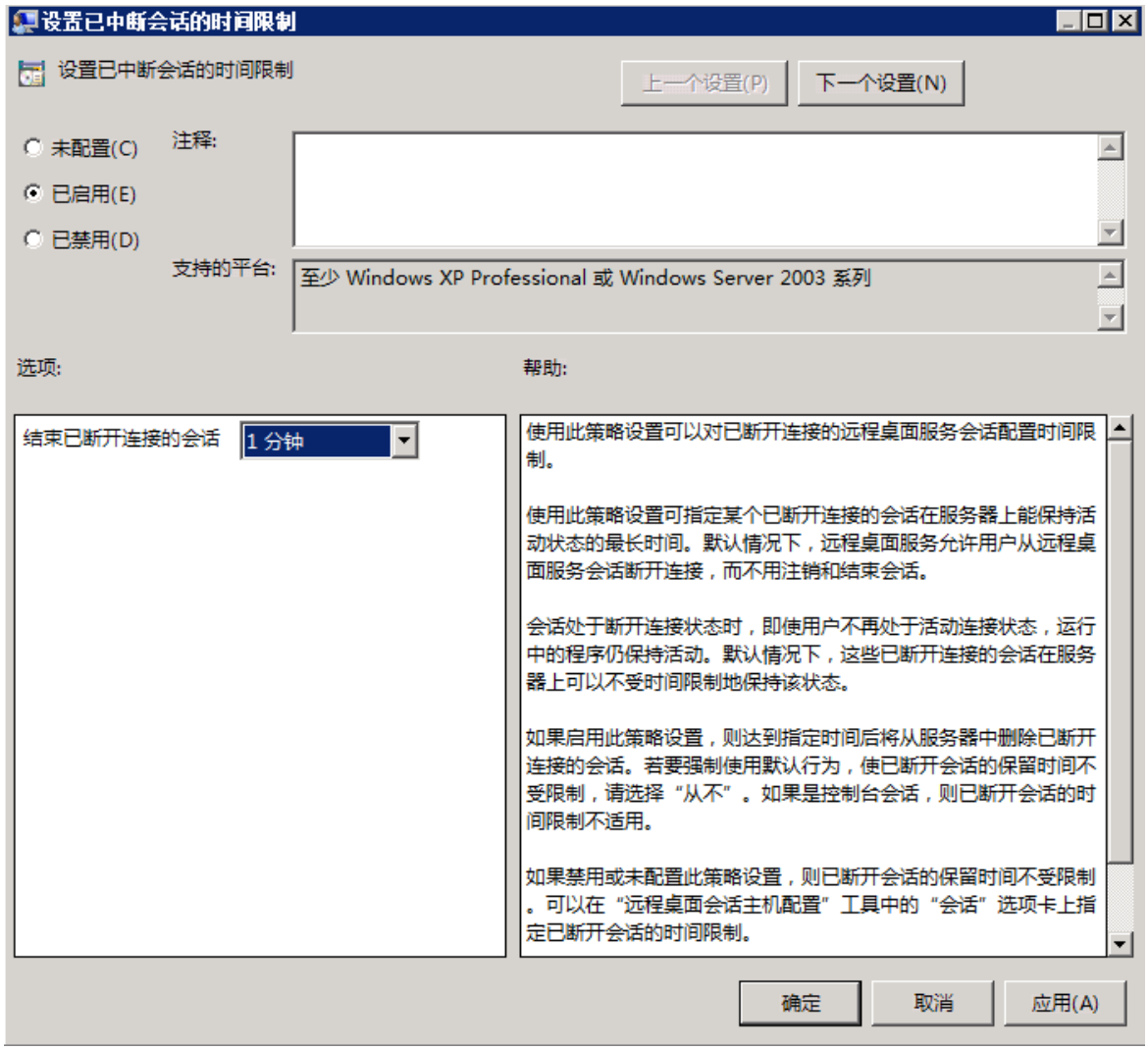
(6) 进入[计算机配置/管理模板/windows 组件/远程桌面服务/远程桌面会话主机/会话时间限制]界面。

图46 本地组策略示意图



(7) 双击<设置已中断会话的时间限制>，在配置界面中选择“已启用”，并设置结束已断开连接的会话为“1 分钟”。

图47 策略配置示意图



单击<确定>即可。

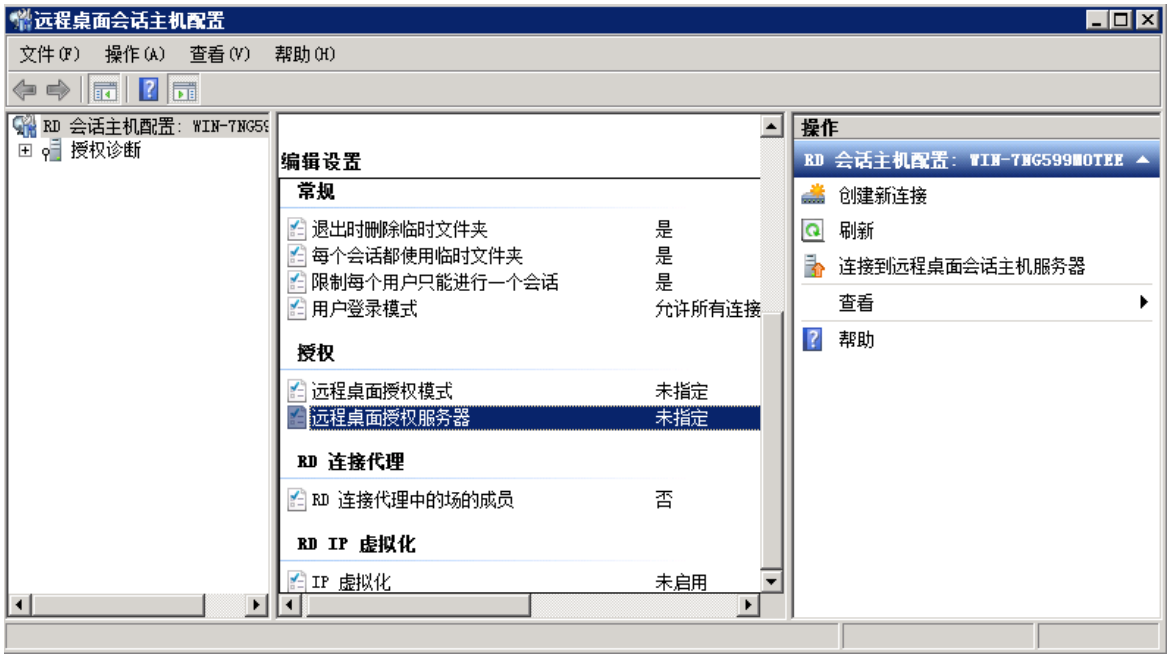
3.3.2 设置RD授权模式

(1) 进入[控制面板/系统和安全/管理工具/远程桌面服务]界面。

图48 远程桌面服务项示意图

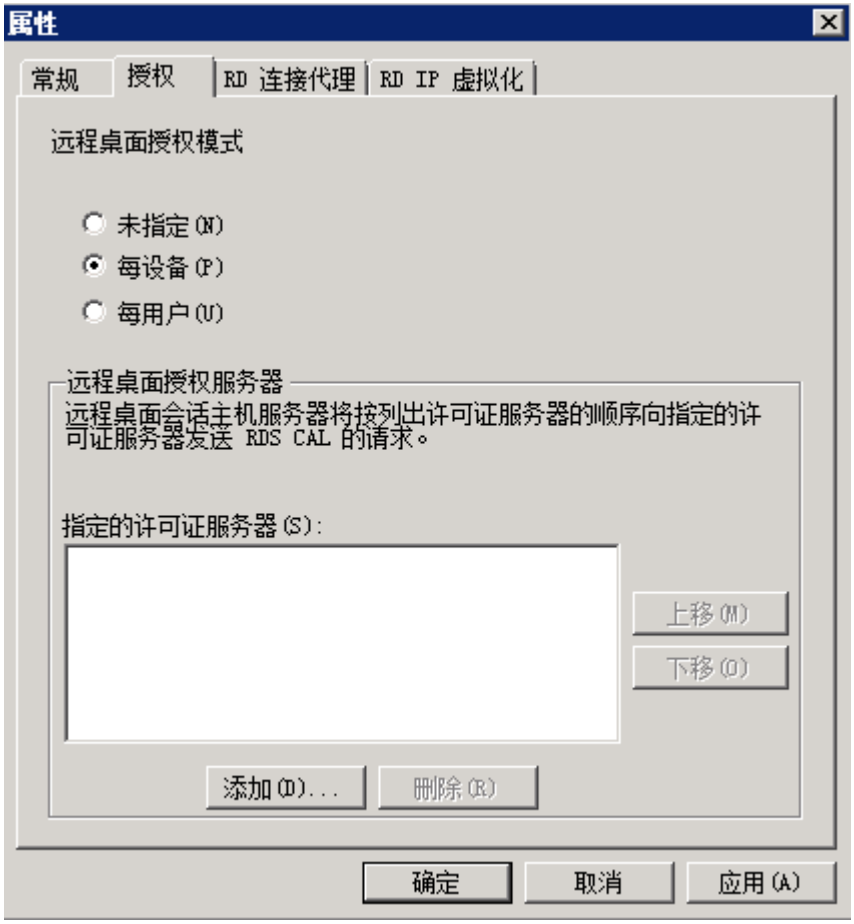
(2) 双击<远程桌面会话主机配置>进入配置界面。

图49 授权诊断示意图



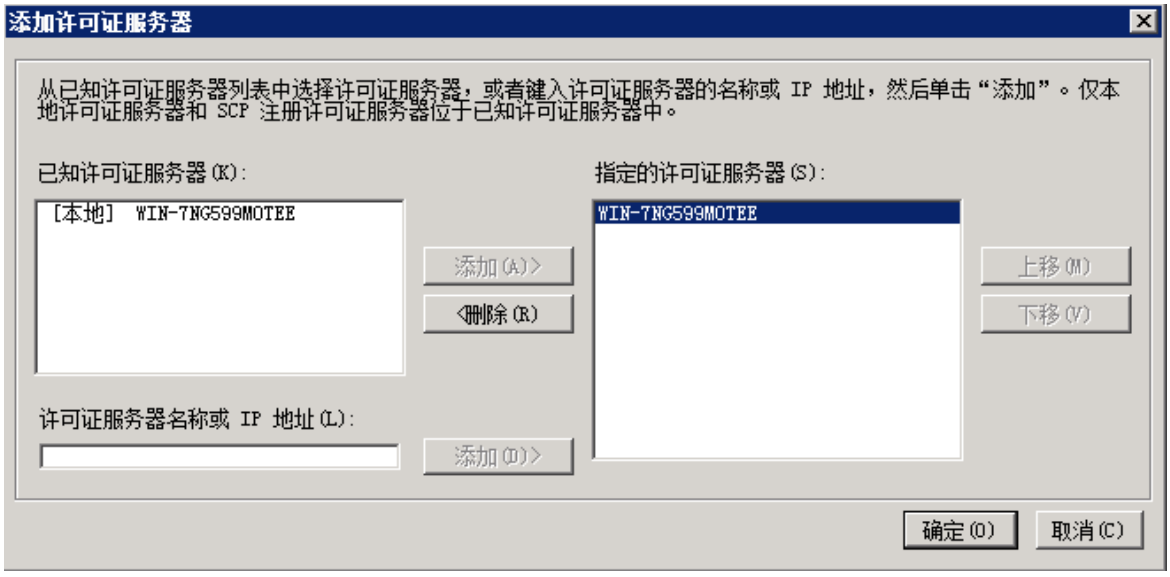
(3) 双击<远程桌面授权服务器>进入配置属性界面，选择“每设备”模式。

图50 授权属性示意图



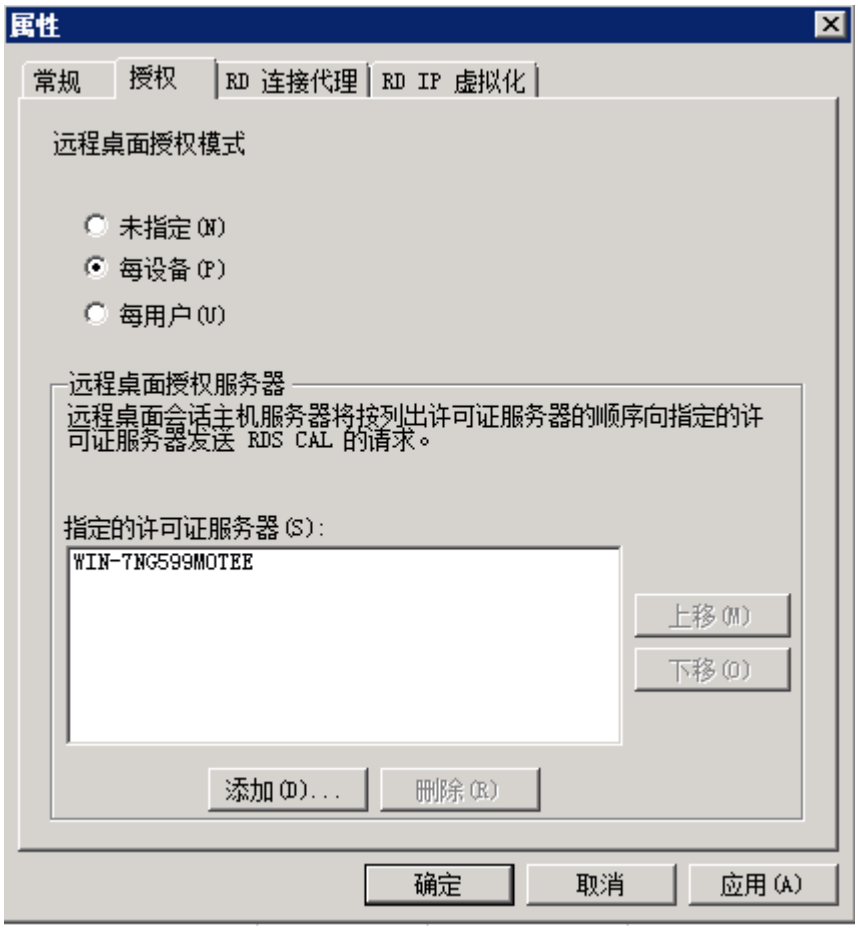
(4) 单击<添加>进入添加许可证服务器界面，将本地服务器添加到指定的许可证服务器中。

图51 添加许可证服务器示意图



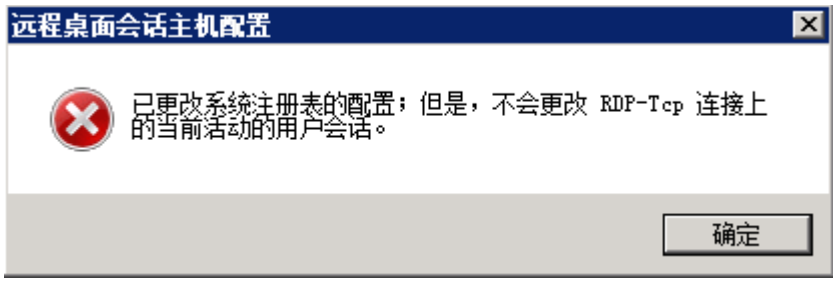
(5) 单击<确定>即可返回配置属性界面。

图52 授权属性示意图



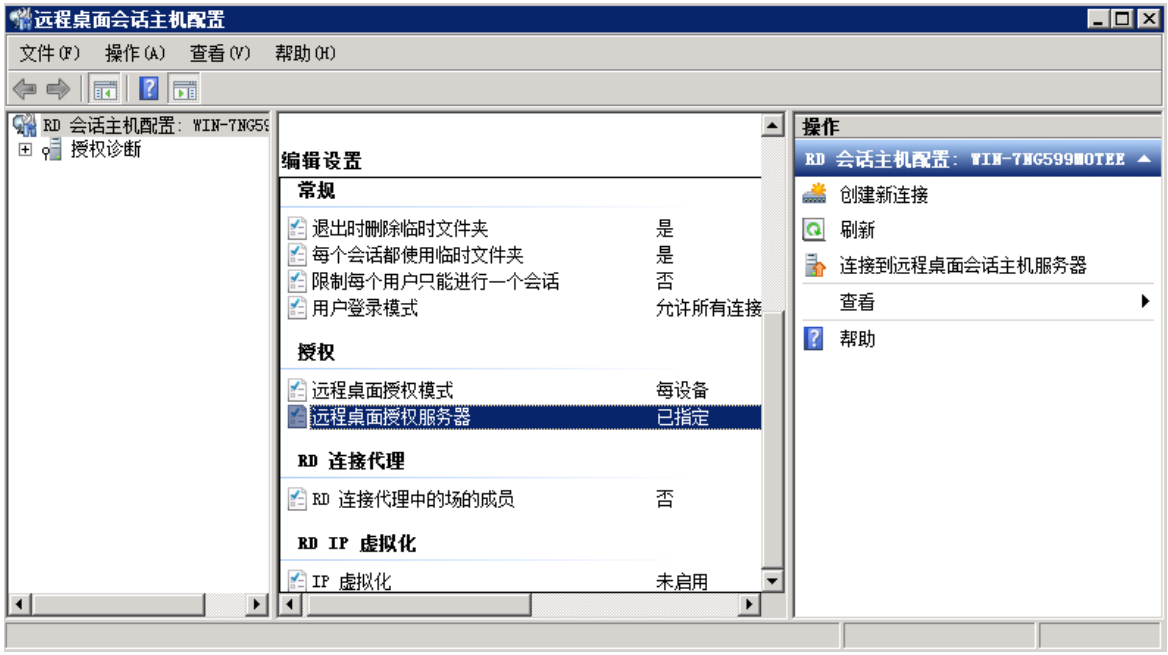
(6) 单击<确定>后提示已更改系统注册表的配置。

图53 远程桌面会话主机配置提示示意图



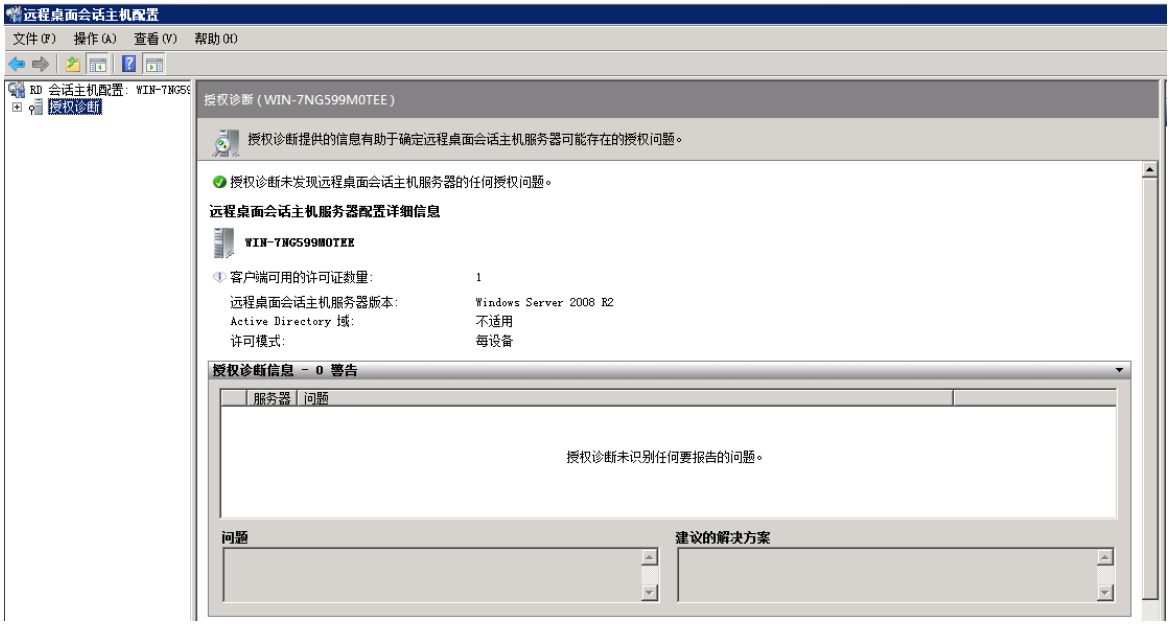
(7) 单击<确定>接口生效，并可以查到配置界面已指定。

图54 授权诊断示意图



(8) 单击<授权诊断>可以看到“授权诊断信息-警告”中为空，表示授权设置正常。

图55 授权诊断示意图



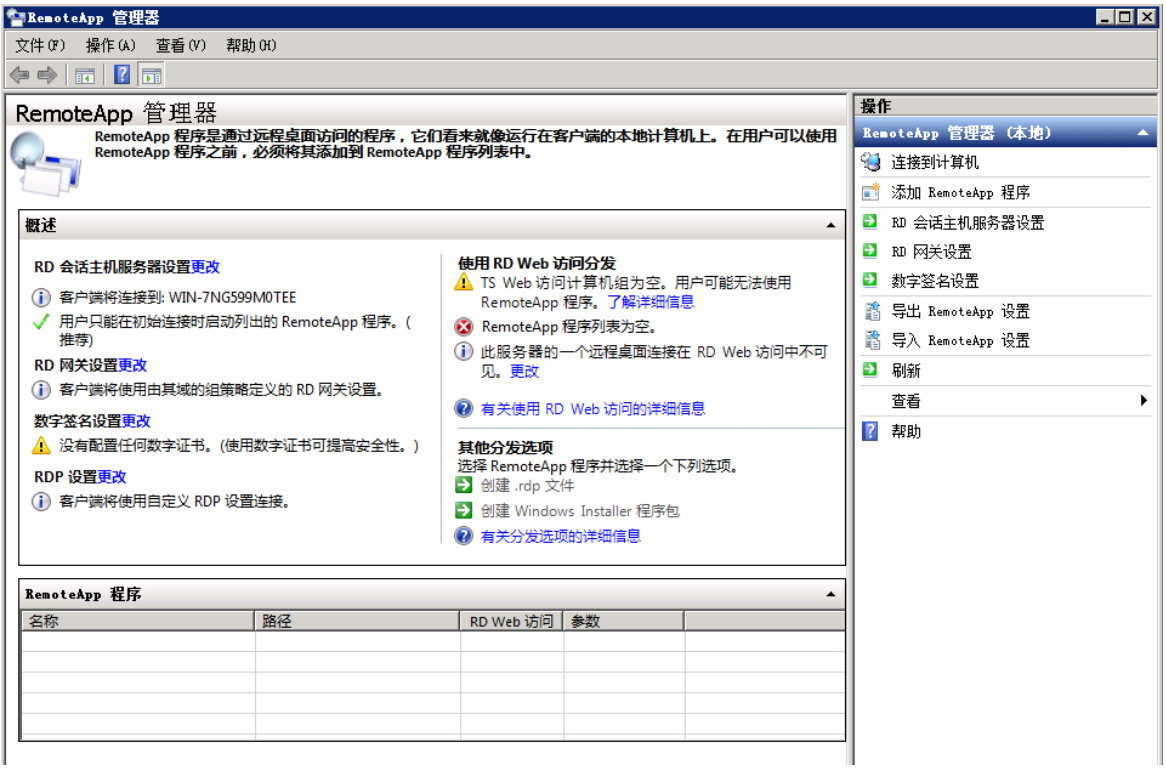
3.3.3 允许用户在初始连接时启动列出和未列出的程序

(1) 进入[控制面板/系统和安全/管理工具/远程桌面服务]界面。

图56 远程桌面服务项示意图

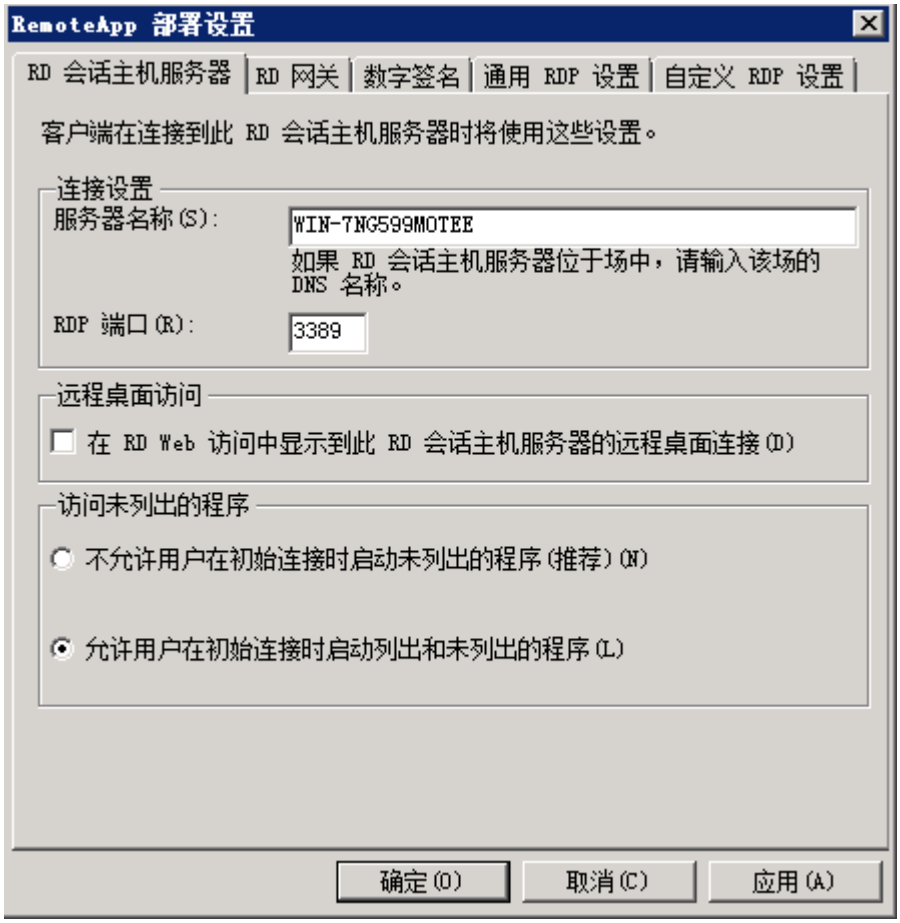
(2) 双击<RemoteApp 管理器>进入配置界面。

图57 RemoteApp 管理器示意图



(3) 单击<RD 会话主机服务器配置更改>进入设置界面，选择“允许用户在初始连接时启动列出和未列出的程序”。

图58 RemoteApp 部署设置示意图

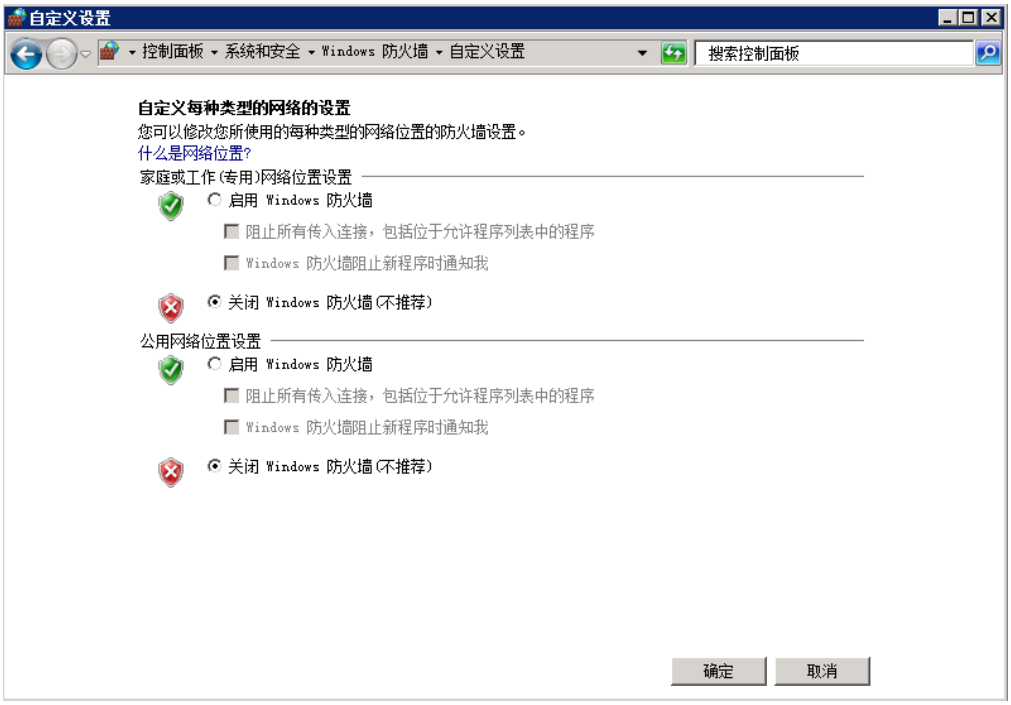


单击<确定>即可。

3.3.4 关闭windows防火墙

进入[控制面板/系统和安全/windows 防火墙/自定义设置]界面，关闭 windows 防火墙。

图59 Windows 防火墙设置示意图



单击<确定>即可。

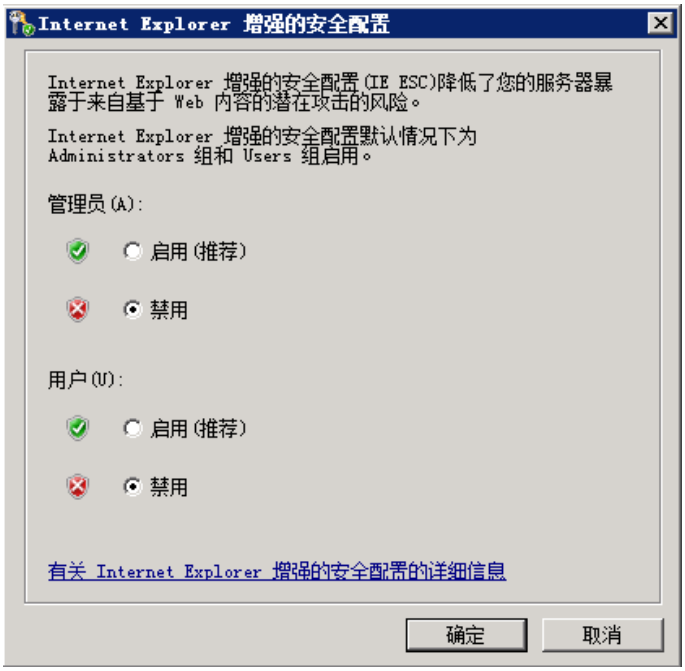
3.3.5 关闭IE增强的安全配置

(1) 进入[服务器管理器]界面。

图60 服务器管理器示意图

(2)　单击<配置 IE SEC>进入 IE 增强的安全配置界面，将管理员和用户禁用。

图61 IE 增强的安全配置示意图



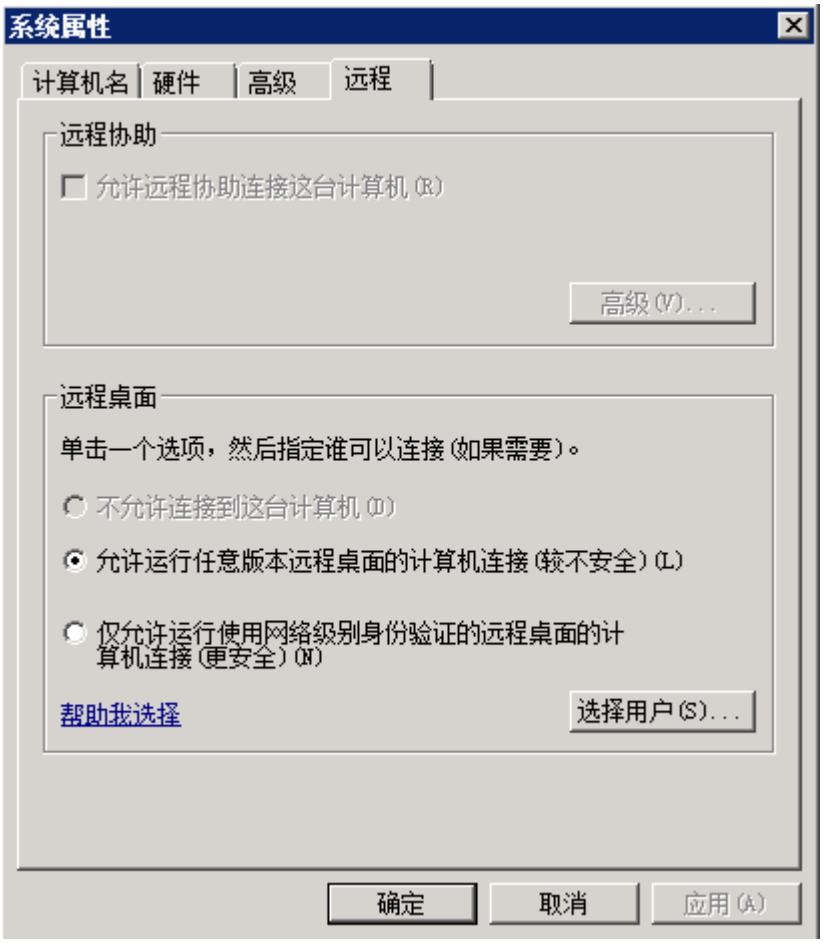
3.3.6 开启远程桌面

(1)　右击计算机，单击<属性>进入系统属性界面。

图62 系统属性示意图

(2) 单击<远程设置>进入远程桌面配置窗口，选择“允许运行任意版本远程桌面的计算机连接(较不安全)”。

图63 远程桌面设置示意图

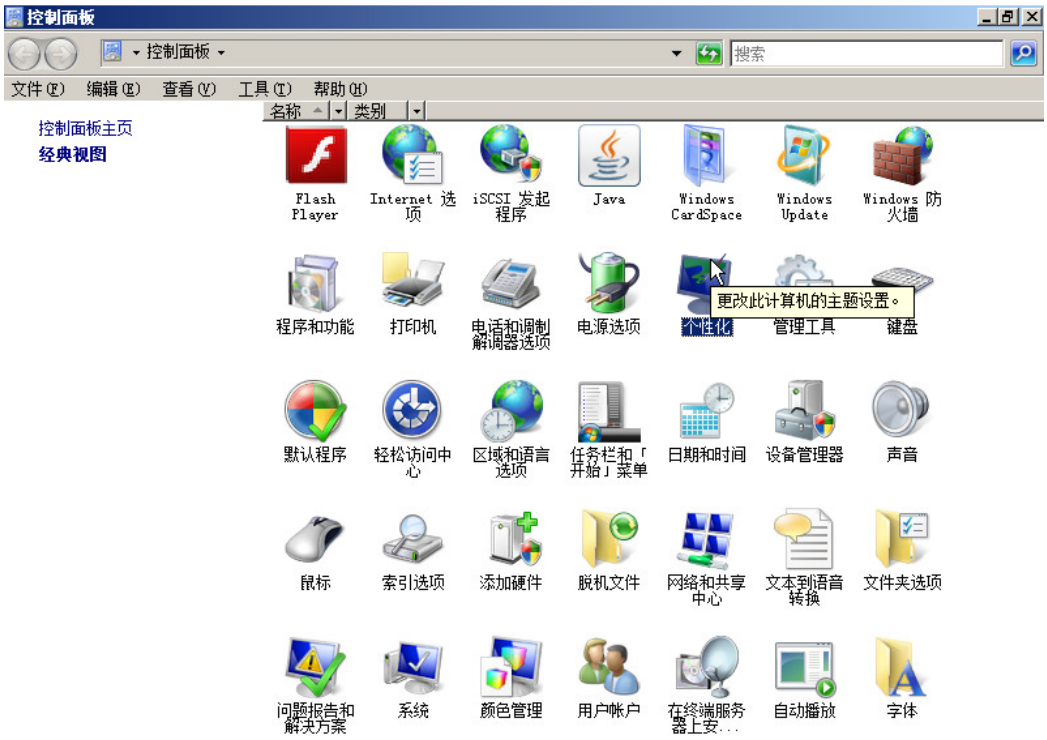


单击<确定>即可。

3.3.7 关闭屏幕保护

(1) 进入“控制面板”中，找到“个性化”。

图64 控制面板示意图

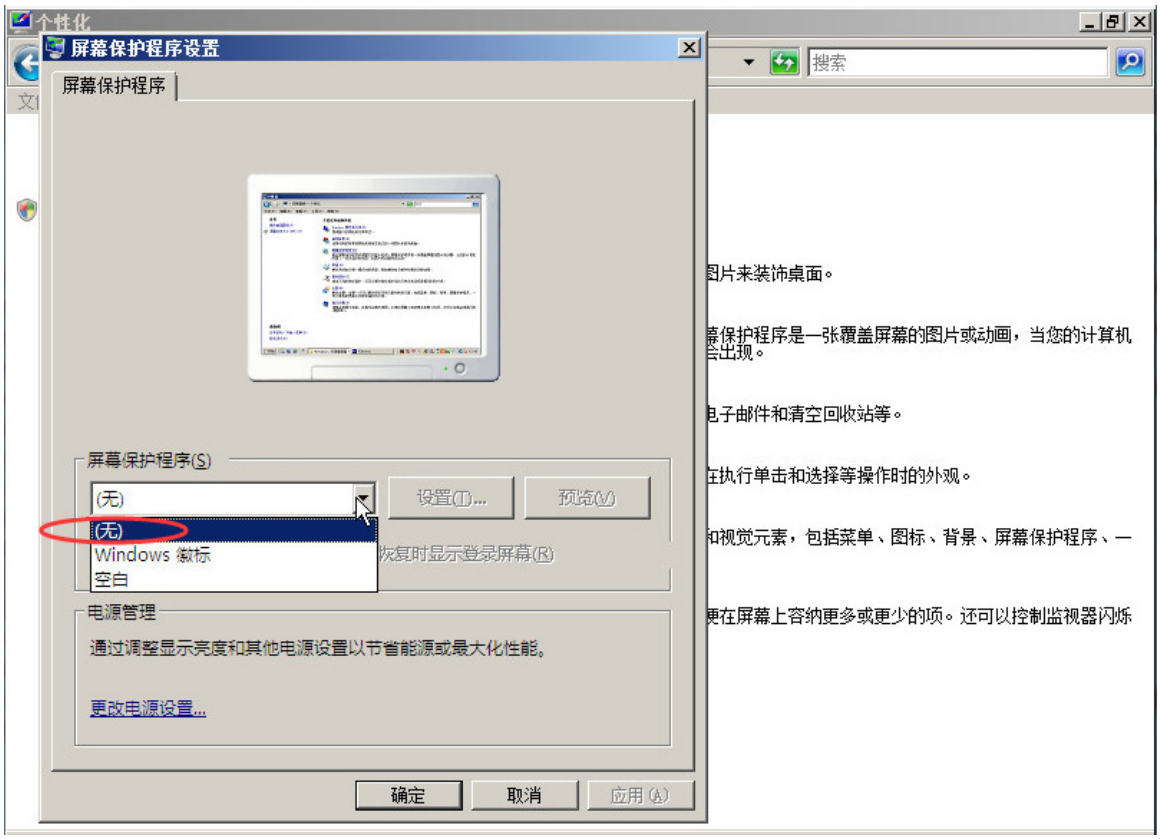


(2) 双击<个性化>后，进入管理界面，找到“屏幕保护程序”。

图65 个性化设置示意图

(3) 双击<屏幕保护程序>后，弹出设置窗口，在“屏幕保护程序”下拉框中选择“(无)”。

图66 屏幕保护程序设置示意图



单击<确定>即可。

(4) 最后，重启应用中心。

3.3.8 启用屏幕保护程序超时

(1) 在运行窗口中输入“gpedit.msc”。

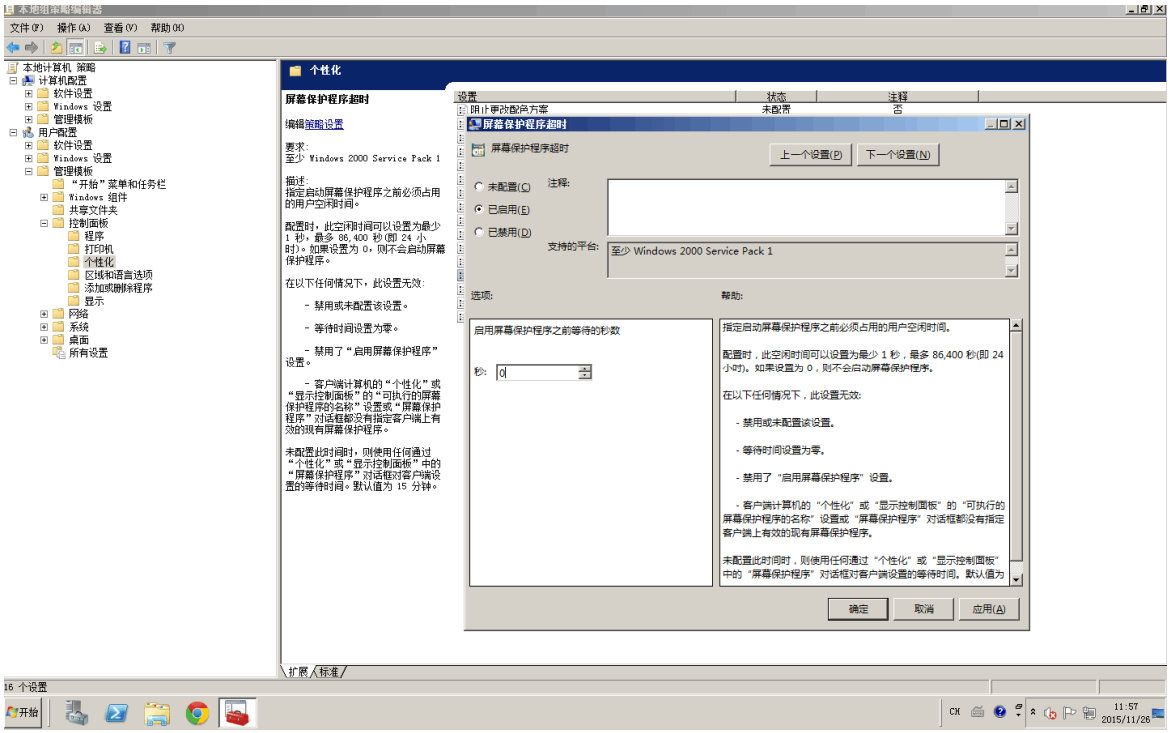
(2) 在本地组策略中，进入[用户配置/管理模板/控制面板/个性化]菜单管理页面。

注意

如果没有[个性化]菜单项，那就找[显示]菜单项。

(3) 找到“屏幕保护程序超时”配置项，编辑为“已启用”，并且将“启用屏幕保护程序之前等待的秒数”设置为“0”秒。

图67 屏幕保护程序超时设置示意图



3.4 在应用中心中安装相关的工具

3.4.1 安装客户端工具

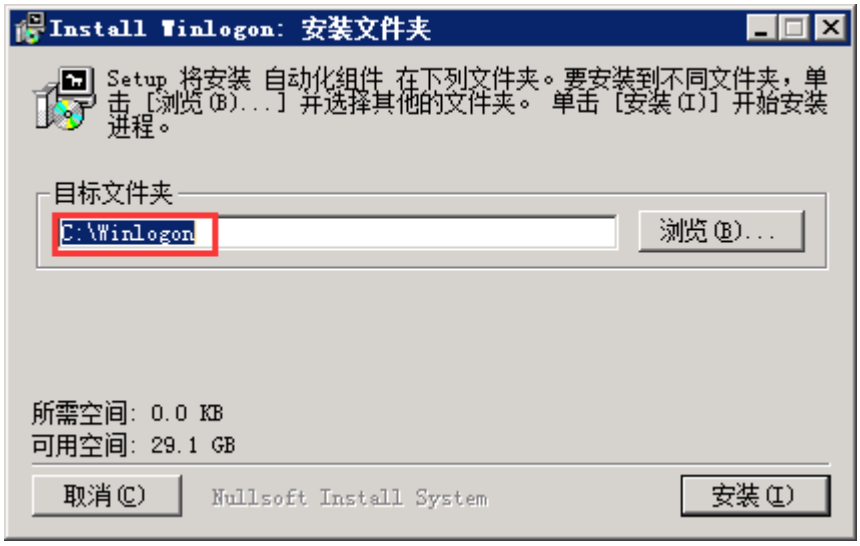
在应用中心中安装需要使用的客户端工具。如：plsql、sqlplus、SQL server management studio、MySQLQueryBrowser、VMware vSphere Client 等。

安装好之后，确保能找到可执行程序的绝对路径，在发布应用的时候，需要填写这些客户端工具的路径。

3.4.2 安装winlogon

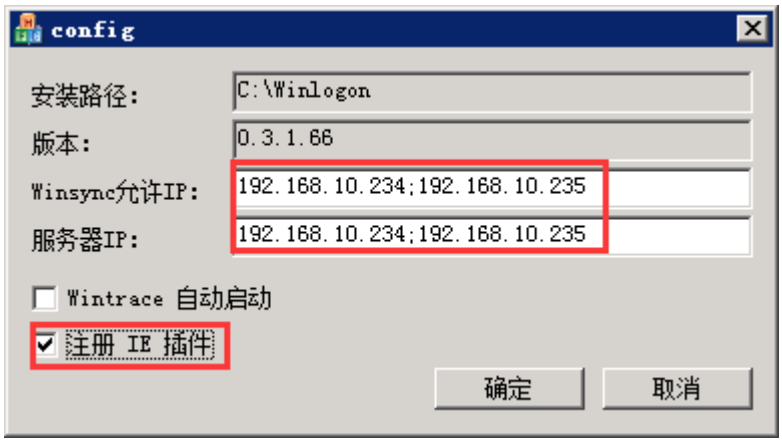
在应用发布服务器使用管理员登录堡垒机，在“工具下载”栏下载 winlogon 安装程序，双击 winlogon 安装程序，选择安装路径（默认即可），点击“安装”，如下图：

图68 安装 winlogon 向导示意图



一直选择默认安装，在“Winsync 允许 IP”和“服务器 IP”栏中填入堡垒机的 ip 地址，如下图：

图69 Winlogon 配置示意图



点击“确定”完成 winlogon 安装。

注意

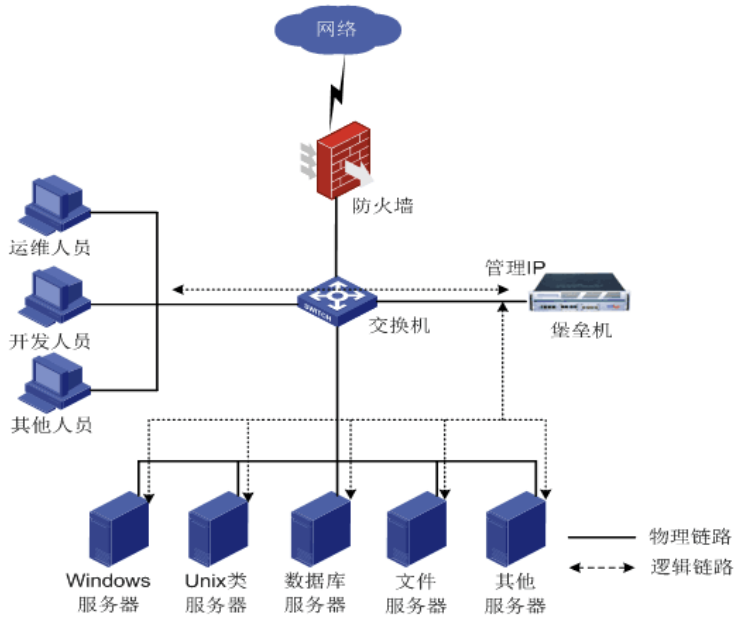
如果有多台堡垒机请用分号间隔各 IP。 如果需发布 IE，请勾选“注册 IE 插件”。勾选之后应用发布服务器上的 IE 浏览器不允许在本地直接使用，必须通过堡垒机的应用发布调用。

4 运维审计系统与应用中心结合使用

用于统一对应用程序进行管理和审计。

4.1 组网需求

图70 应用发布配置组网示意图



4.2 系统版本要求

适用产品版本： ESS 6102

4.3 运维审计系统添加应用发布服务器

利用配置管理员登录堡垒机，在“基本控制”>“目标设备”界面中先将应用发布服务器做为普通的 Windows 设备添加到堡垒机，然后编辑应用发布服务器，在服务列表中编辑“RDP”服务，如下图：

图71 编辑应用发布服务器 RDP 服务示意图

将“应用发布服务器”勾选上，点击“测试连接”之后，堡垒机会自动获取应用发布服务器上的 Winlogon 信息（版本、路径），如下图：

图72 应用发布服务器 winlogon 测试连接示意图

同步：若勾选此选项，堡垒机会在应用发布服务器上创建和普通用户同名的系统账号。当普通用户访问应用程序时，登录该应用发布服务器都使用各自的同名系统账号，密码由堡垒机随机产生并完成登录。

图73 勾选同步用户示意图

若未同步成功，管理员可以在应用发布服务器的基本信息配置页面手动点击同步，如下图：

图74 手动同步用户密码示意图

注意

堡垒机需要访问应用发布服务器 TCP/5156 端口，如果此处获取不到 winlogon 版本和路径信息，请检查 Winlogon 配置页面堡垒机地址是否填写正确，以及应用发布服务器防火墙是否允许该服务端口。

4.4 C/S应用发布

4.4.1 发布应用

新建目标设备之后添加 rdpapp 服务，配置方法如下图所示：

图75 C/S 应用发布 rdpapp 服务示意图

- 名称：该应用程序的名称。
- app 类型：这里选择 general。
- Winlogon：“应用程序”一栏填入应用程序的绝对路径。
- RemoteApp 程序：填入 slrdp。
- 其余选项类似 rdp 服务的配置，这里不再重复介绍。

⚠ 注意

少数应用程序除了需要填写绝对路径还需要填写工作目录和参数，请参考应用程序的快捷方式的属性进行设置。

4.4.2 密码代填

对于一些需要登录认证的应用程序，堡垒机提供了一套自动登录的机制来完成用户认证信息的填写。用户在设备列表中选择应用程序和相应的系统账号之后，堡垒机会在应用发布过程中自动填写登录页面的用户名和密码等相关信息。

1. 兼容列表

应用程序账号密码代填兼容版本信息如下表所示：

表8 B/S 应用程序账号密码代填兼容列表

类别	软件	已适配的版本
Oracle客户端	SQL PlusW	Oracle Client 9i
		Oracle Client 10g
	Pl/SQL Developer	7.1
		9
		10
		11
	Toad for Oracle	9.7
		10.5
SQL Server客户端	SQL Server 查询分析器	2000
	SQL Server Management Studio	2005简易版中文
		2008简易版中文
		2005中文
		2008中文
		2012中文
DB2客户端	Quest Central for DB2	V5.0英文
VMware客户端	VMware vSphere Client	5.5 中文
	VMware vSphere Client	6.0 中文
其它	Radmin	3.4 中文版
	PowerBuilder	9.0 企业版

注意

内置 cs 代填脚本是根据可执行文件名进行代填脚本的匹配，同一个应用存在多个版本时，默认启用了最高版本的代填脚本，如果要使用低版本的应用，管理员可以在“策略配置”>“密码代填”栏进行修改。

2. 一般应用密码代填举例

新建目标设备之后添加 rdpapp 服务，配置方法如下图：

图76 一般应用密码代填 radapp 服务示意图

其中“名称”填入需要访问的ip地址，“Winlogon应用程序”中填写vsphere的绝对路径，“RemoteApp程序”中填写 slrdp。

接着在“密码管理”页面中配置好 vsphere 登录的账号及密码，配置好访问权限后使用普通用户即可登录，如下图：

图77 一般应用密码代填登录界面示意图

可以看到，ip 地址、用户名以及密码已经被自动填入并且已经自动开始登录，如下图：

图78 一般应用密码代填结果示意图

3. Oracle应用密码代填

新建目标设备之后添加 rdpapp 服务，配置方法如下图：

图79 Oracle 应用 radapp 服务示意图

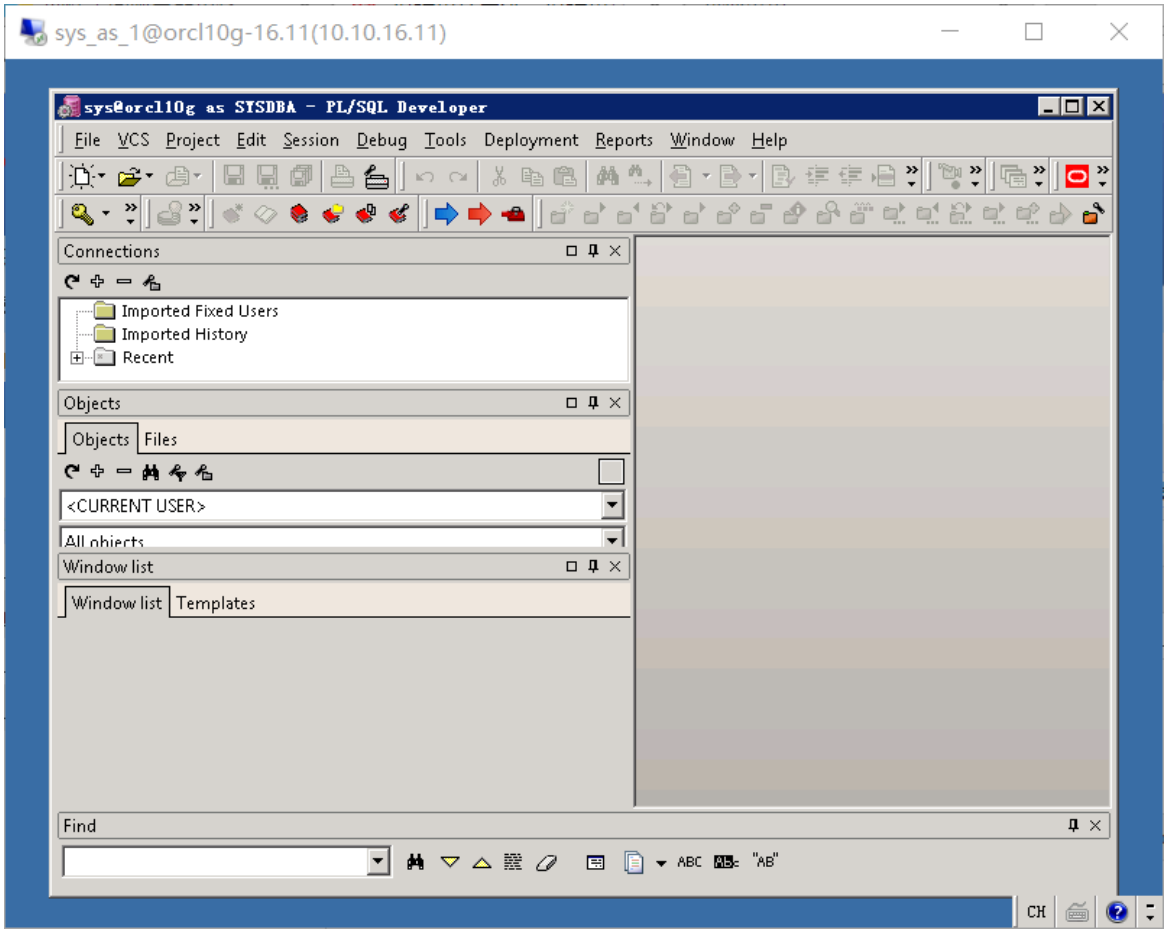
其中“名称”填入需要访问的数据库名称，“Winlogon 应用程序”中填写 plsqldev.exe 程序的绝对路径，“RemoteApp 程序”中填写 slrdp。

接着在“密码管理”页面中配置好登录 oracle 数据库的账号及密码，配置好访问权限使用后普通用户即可登录，如下图：

图80 Oracle 应用密码代填登录示意图

成功进入界面即为代填成功，如下图：

图81 Oracle 应用密码代填结果示意图



- Oracle 系统账号说明

Oracle 类型的应用发布系统账号比较特殊，堡垒机在原有系统帐号的基础上做了扩展，扩展方式为“原账号_as_登录角色代码”，（其中 as_0 代表角色为“normal”的 oracle 帐号，as_1 代表角色为“sysoper”，as_2 代表角色为“sysdba”）例如：

oracle 的管理员账号为“sys”，该帐号在用 plsql 登录的时候要选择角色为“sysdba”，所以我们要新建一个名为“sys_as_2”的系统帐号。

图82 Oracle 系统账号说明示意图

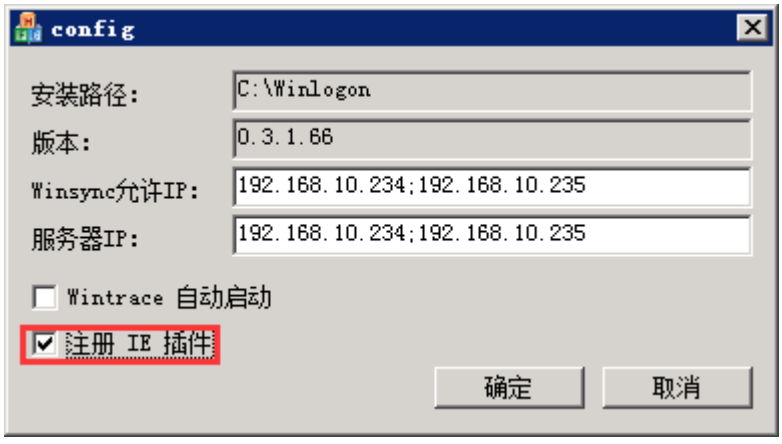
4.5 B/S应用发布

4.5.1 IE浏览器

1. Winlogon配置

通过 IE 浏览器来访问的系统，我们需要通过 http 类型的应用发布来进行访问。需要开启 Winlogon 的“注册 IE 插件”功能，如下图所示：

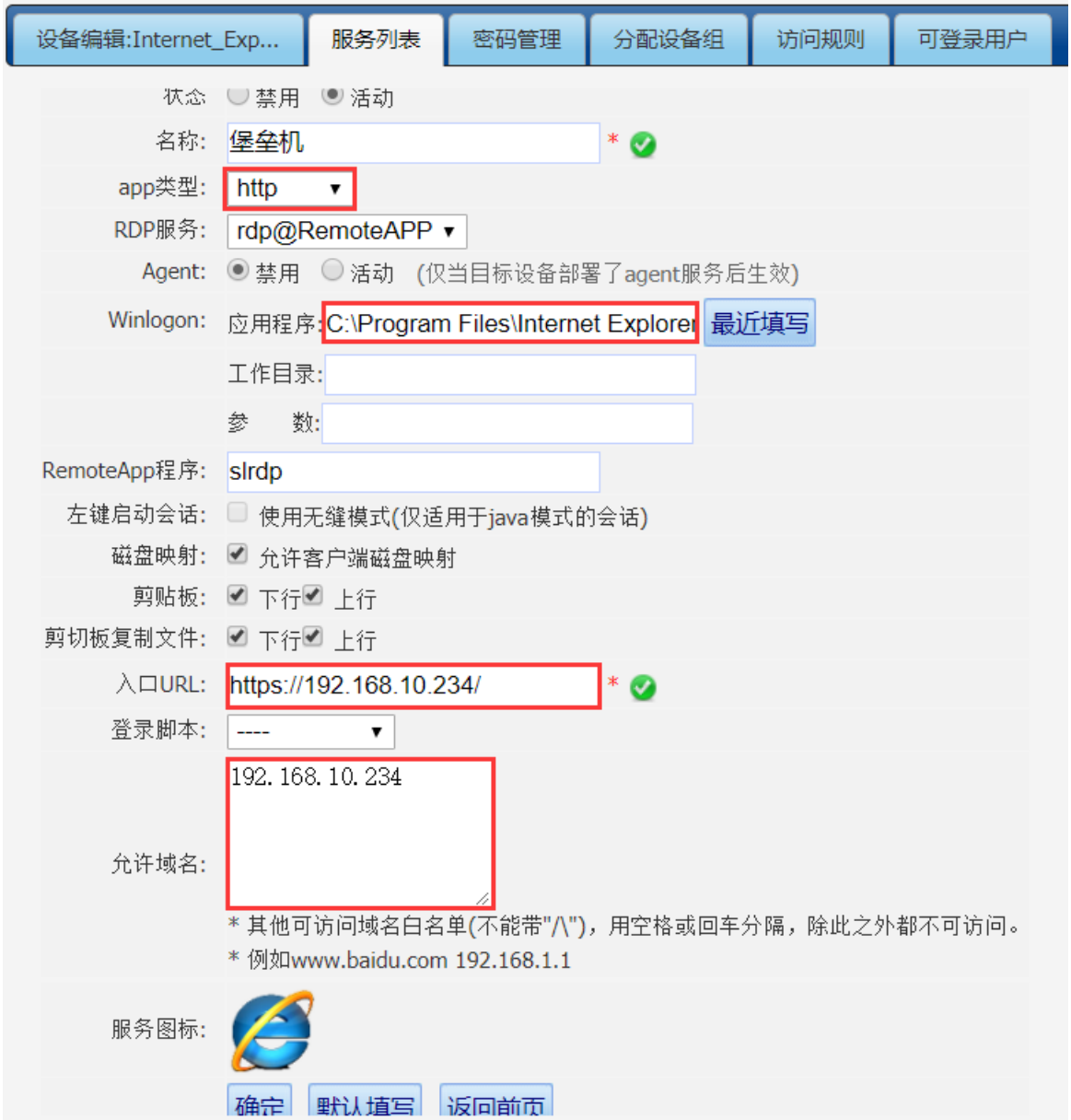
图83 注册 IE 插件示意图



2. 发布应用

新建目标设备之后添加 rdpapp 服务，配置方法如下图：

图84 B/S 应用发布 rdpapp 服务示意图



- 名称：该应用程序的名称。
- App 类型：本节介绍 http 方式，这里选择 http。
- Winlogon：“app 类型”选择 http 之后“应用程序”一栏会自动填上 IE 浏览器的路径。
- RemoteApp 程序：填入 slrdp。
- 入口 URL：填入要访问的 URL 链接
- 允许域名：填上允许访问的 ip 地址或者域名（格式参考下面的说明文字）。
- 其余选项类似 rdp 服务的配置，这里不再重复介绍

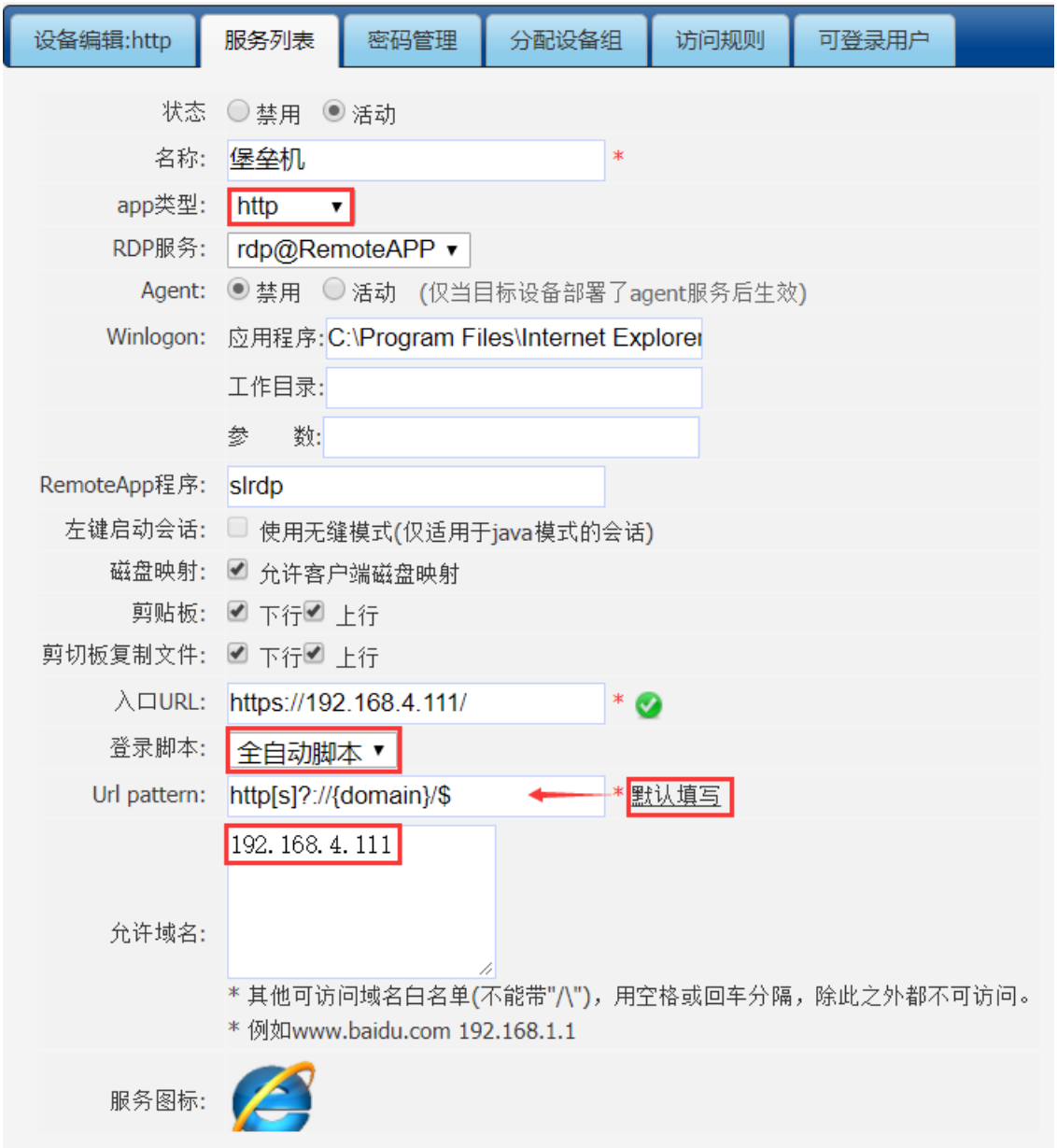
配置好访问权限之后便可直接访问，访问过程中 IE 浏览器会自动跳转至配置好的 URL。

3. 密码代填

- 全自动脚本

全自动脚本是 HTTP 类型密码代填中最简单配置的方式，编辑相关服务，如下图：

图85 http 类型配置全自动脚本登录示意图



选择登录脚本为“全自动脚本”。

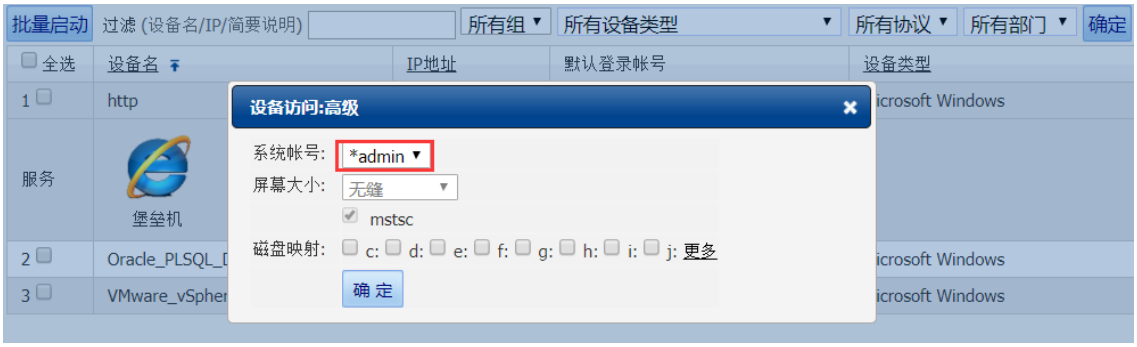
填写网页匹配的 Url pattern，可以点击“默认填写”生成左边的默认 Url pattern，Url pattern 是指 HTTP 类型密码代填中的匹配。

注意

- 当 Url pattern 匹配网页的 URL 时，堡垒机就会提交用户名、密码进行代填操作，所以需要确定。Url pattern 不能匹配成用户登录成功后的网页 URL，否则堡垒机就会一直尝试代填。
- Url pattern 采用的是正则表达式的结构。

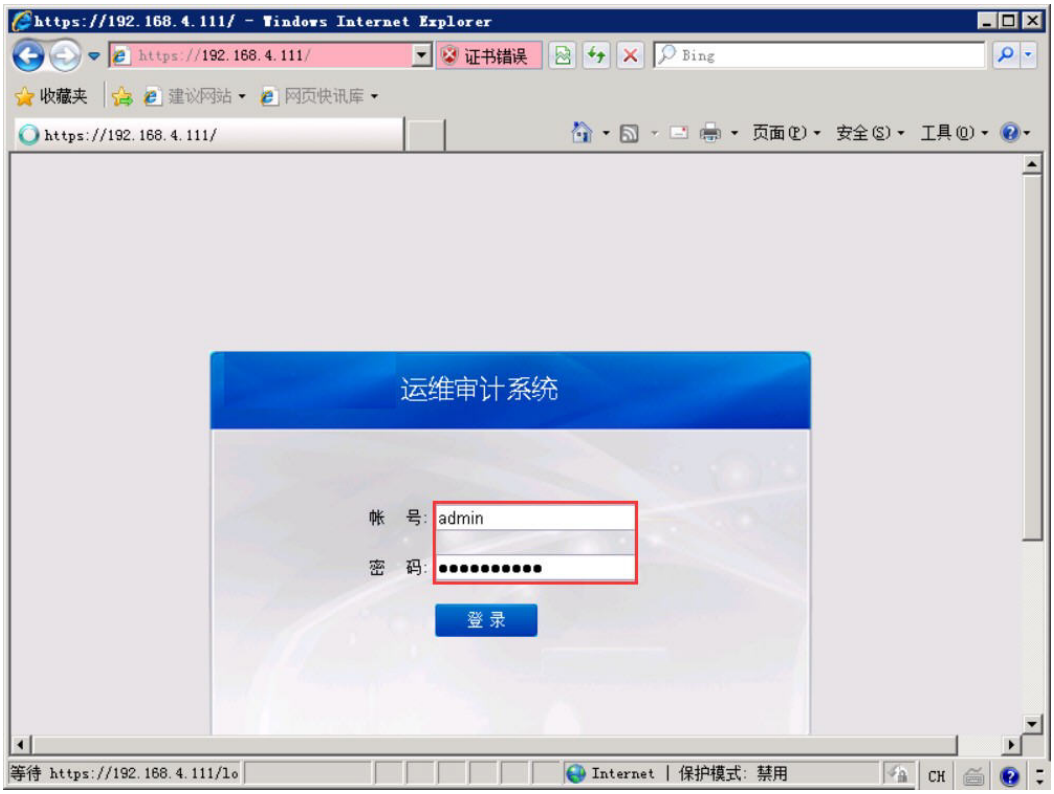
进入“密码管理”菜单，托管账号密码，并分配相应的权限，直接使用普通用户进行登录测试，如下图：

图86 http 类型配置全自动脚本登录页面示意图



登录网页进行了账号密码代填并成功进入网页，即为成功，如下图：

图87 http 类型配置全自动脚本登录成功示意图



注意

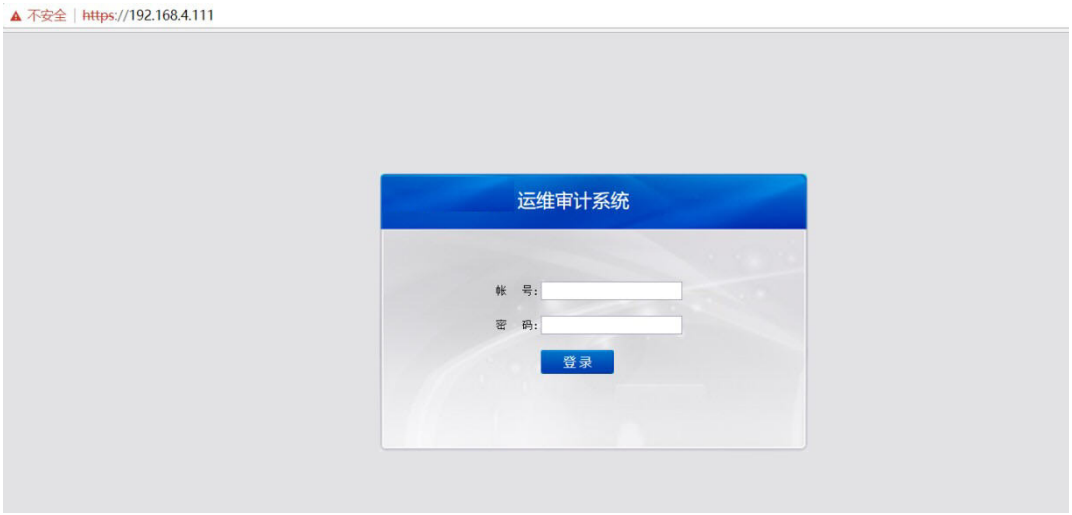
因为登录测试不允许进行操作，如果遇见“证书错误”等需要先进行交互式操作才能出现登录页面的，请先建立访问权限，然后用普通用户测试。

- 半自动脚本

使用半自动脚本方式，需要获取登录界面 html 的标签属性，配置比全自动复杂。

首先使用浏览器，访问目标设备页面，如下图：

图88 http 类型半自动脚本登录页面示意图



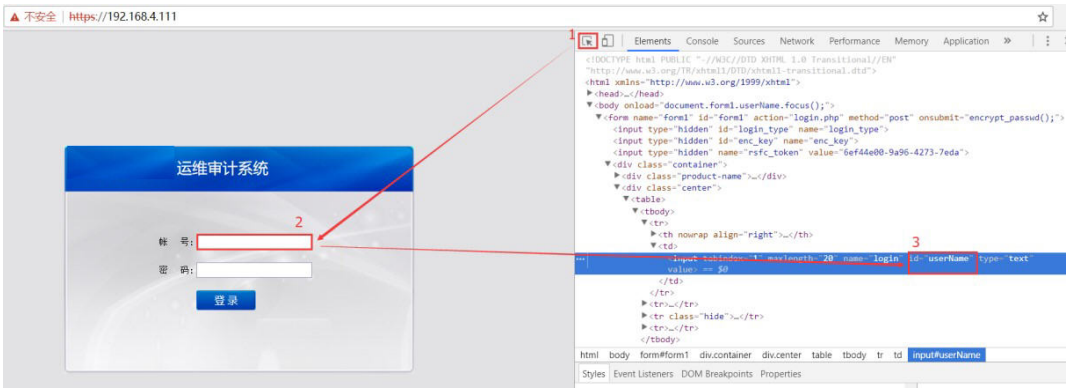
接着点击键盘“F12”，打开浏览器开发人员调试工具，如下图：

(1) 点击“选择元素”按钮。

(2) 将鼠标移动到用户名输入框后单机。确认该元素被锁定。

(3) 查看该 html 元素的属性。其中需要获取“name”字段属性或者“id”字段属性。

图89 http 类型半自动脚本页面元素示意图



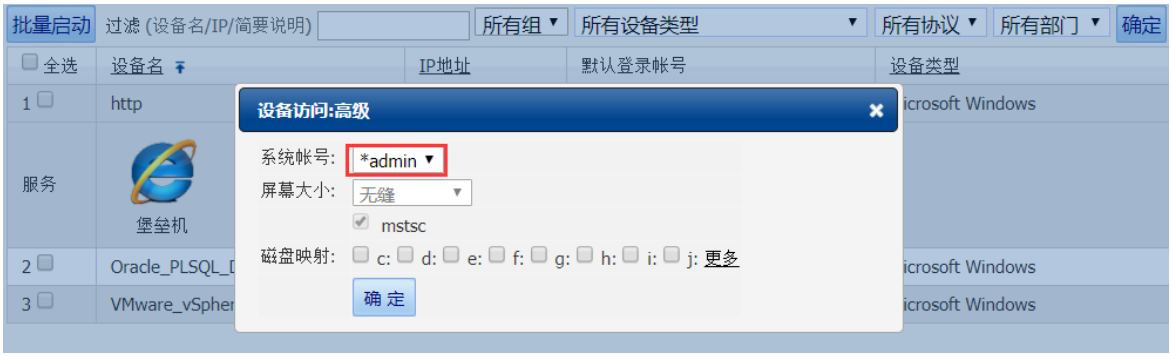
以同样的方式获取密码框和登录按钮的“name”或者“id”属性，编辑相关服务，如下图：

图90 半自动脚本服务配置示意图

- 选择登录脚本为“半自动脚本”。
- 填写网页匹配的 Url pattern，可以点击“默认填写”生成左边的默认 Url pattern。
- 编辑“用户名框标识”，“密码框标识”，“提交按钮标识”为上一步获取到的内容。

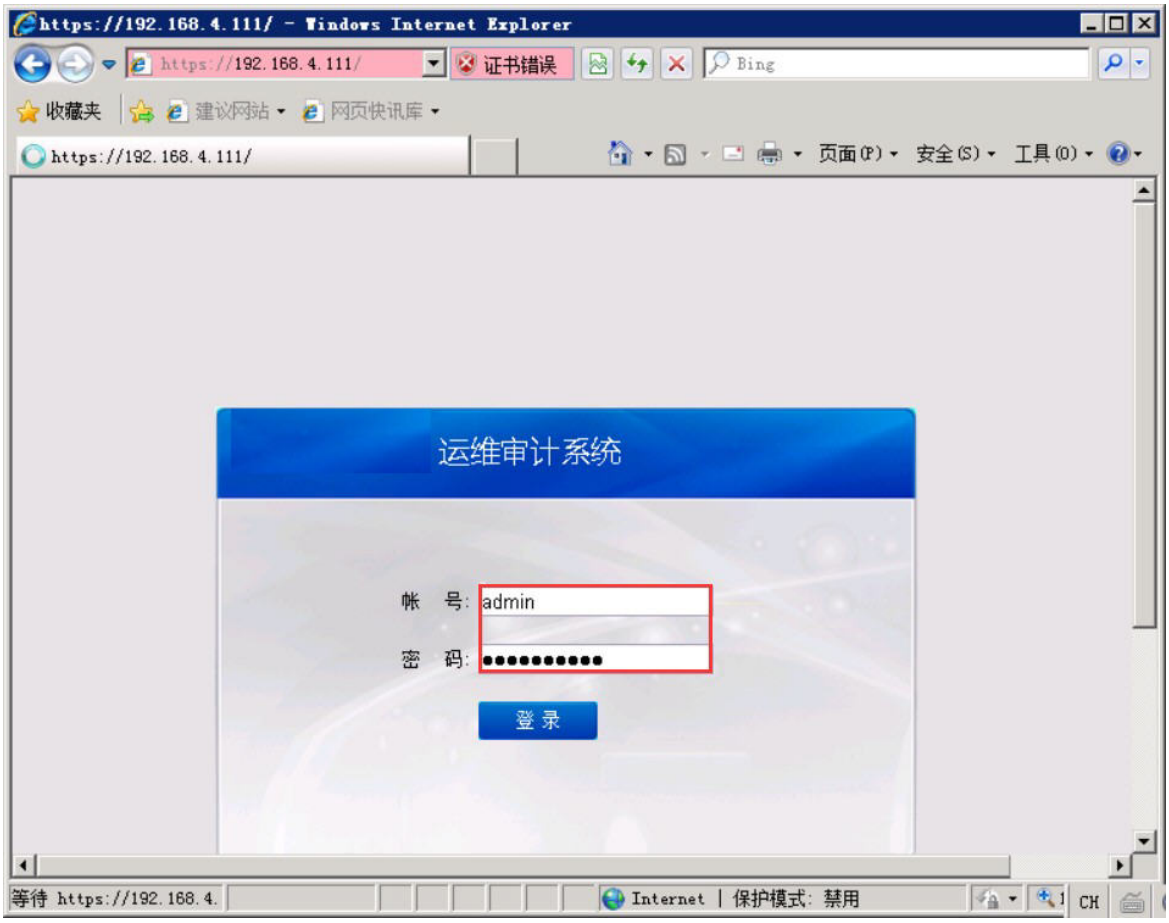
接着进入“密码管理”，托管账号密码，并分配相应的权限，直接使用普通用户进行登录测试。

图91 半自动脚本登录测试页面示意图



登录网页进行了账号密码代填并成功进入网页，即为成功。

图92 半自动脚本登录测试成功示意图



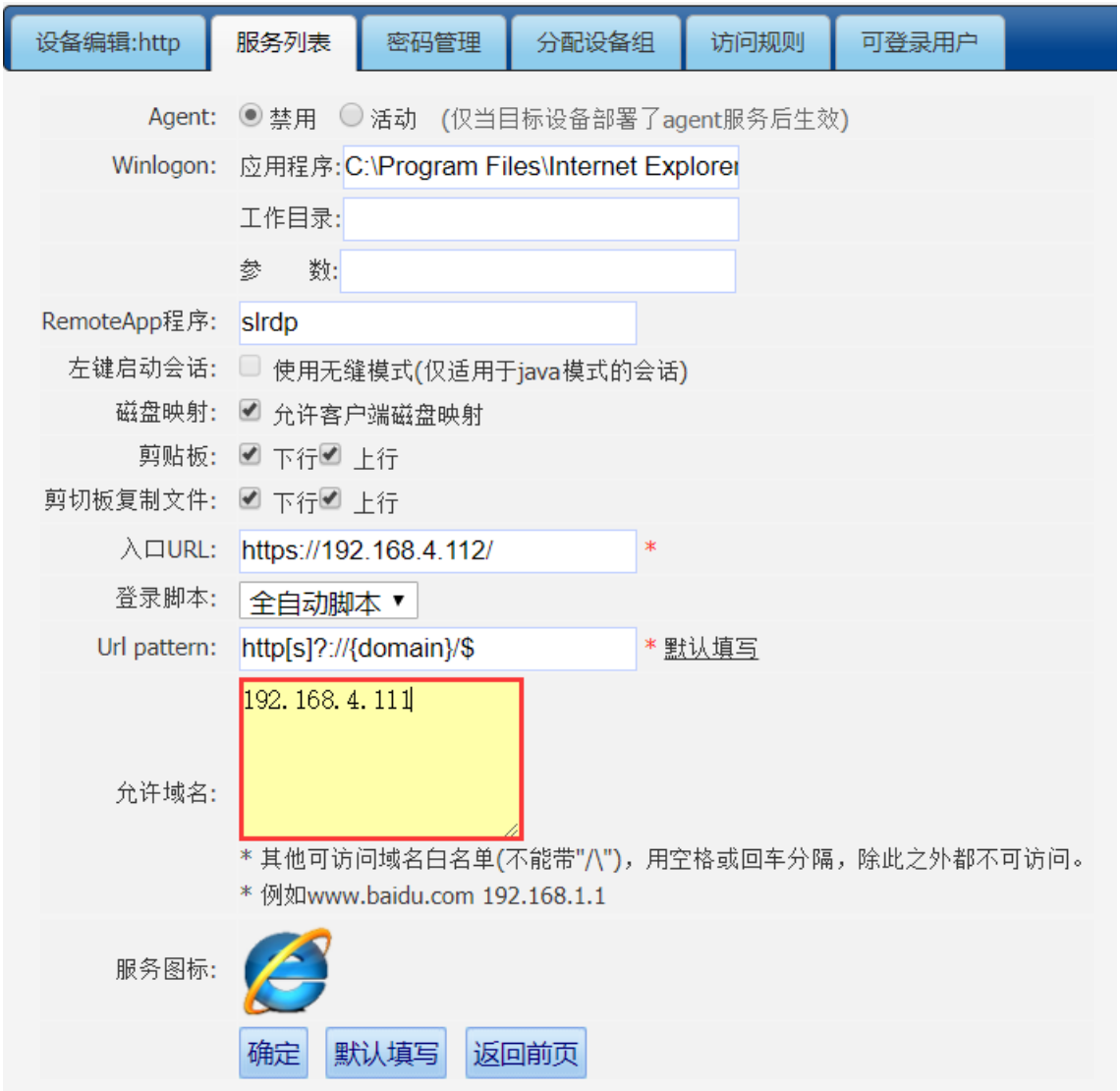
注意

B/S 应用的密码代填仅支持 form 表单有明确的 id 或者 name，无验证码，登录按钮没有绑定特殊 JavaScript 事件的情况。

- URL 限制

IE 浏览器可以做 URL 限制，在允许域名栏填入允许访问的 IP 或域名白名单，如下图：

图93 IE 浏览器 URL 限制示意图



4.5.2 Chrome浏览器

1. 准备条件

Chrome 浏览器用于支持 vSphere_Web_Client 密码代填，在应用发布服务器上需配置以下内容：

(1) 安装 jave8：需要确保系统环境变量中包含 Java 的路径需要确保系统环境变量中包含 Java 的路径

(2) 安装 Chrome 浏览器：Chrome v59 至 v61 之间的版本

(3) 安装.net3.5

2. 发布

新建目标设备之后添加 rdpapp 服务，配置方法如下图：

图94 Chrome 类型 radapp 服务示意图

- 名称：该应用程序的名称
- App 类型：本节介绍 Chrome 方式，这里选择 Chrome。
- RDP 服务：配置应用发布服务器及登录该应用发布服务器的系统账号，若之前配置应用发布服务器勾选了“同步”则这里只需要选择应用发布服务器。
- Winlogon：“应用程序”一栏填入 Chrome 浏览器的绝对路径。
- RemoteApp 程序：不填
- 入口 URL：填入要访问的 URL。
- 登录模式：不带填、自动和高级三种模式

配置好访问权限之后便可直接访问，访问过程中 Chrome 浏览器会自动跳转至配置好的 URL。

3. 密码代填

- chrome 类型自动代填

自动寻找需要代填的用户名，密码框和提交按钮，该模式只能处理简单场景，可适用于 vSphere_Web_Client 密码代填

编辑目标设备 rdpapp 服务，配置方法如下图：

图95 Chrome 类型密码自动代填 radapp 服务示意图

其中登录模式选择“自动”，其它参考 chrome 类型的发布。

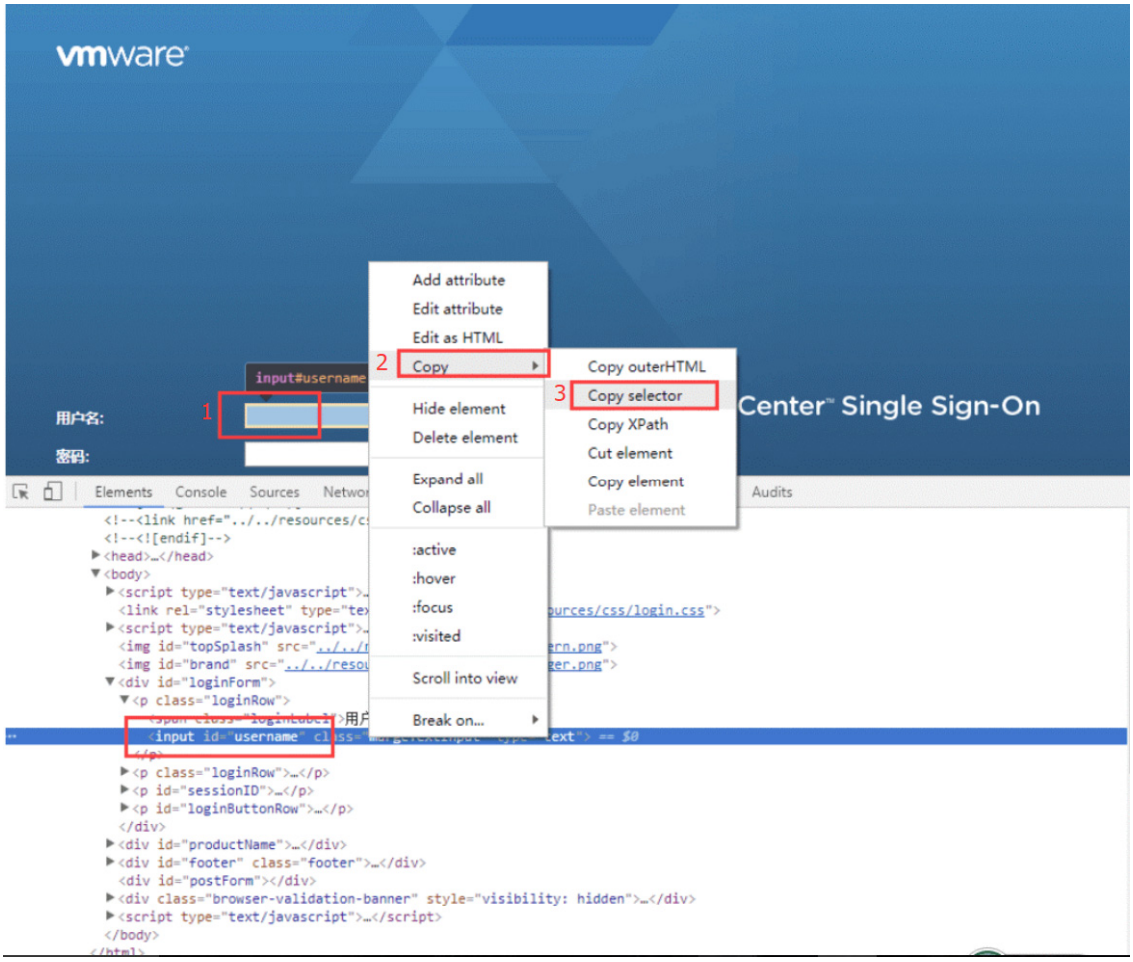
- 高级代填

如果自动代填没有代填成功，可以使用高级代填配配置，编辑目标设备 rdpapp 服务，配置方法如下图：

图96 Chrome 类型密码高级代填 radapp 服务示意图

登录模式：选择“高级”，填入用户名框、密码框、提交按钮标识（都为 css 选择器），右击页面“用户框 > copy > copy selector”，具体操作如下图所示：

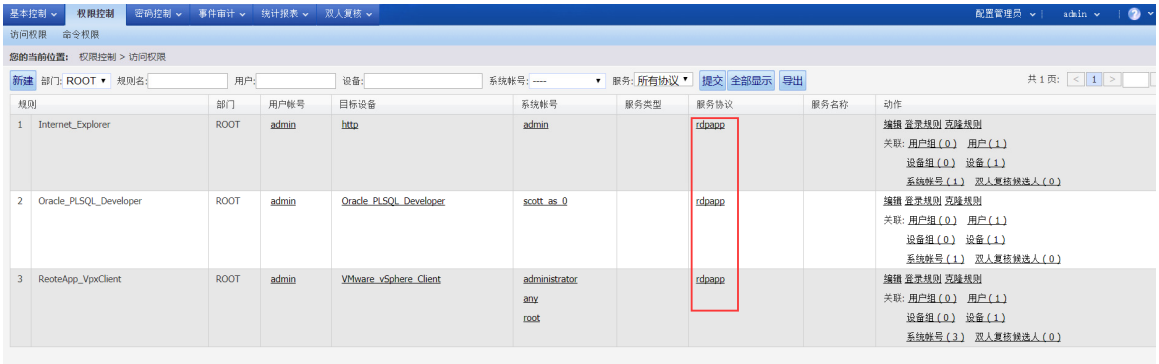
图97 Chrome 类型密码代填高级模式示意图



4.6 配置访问权限

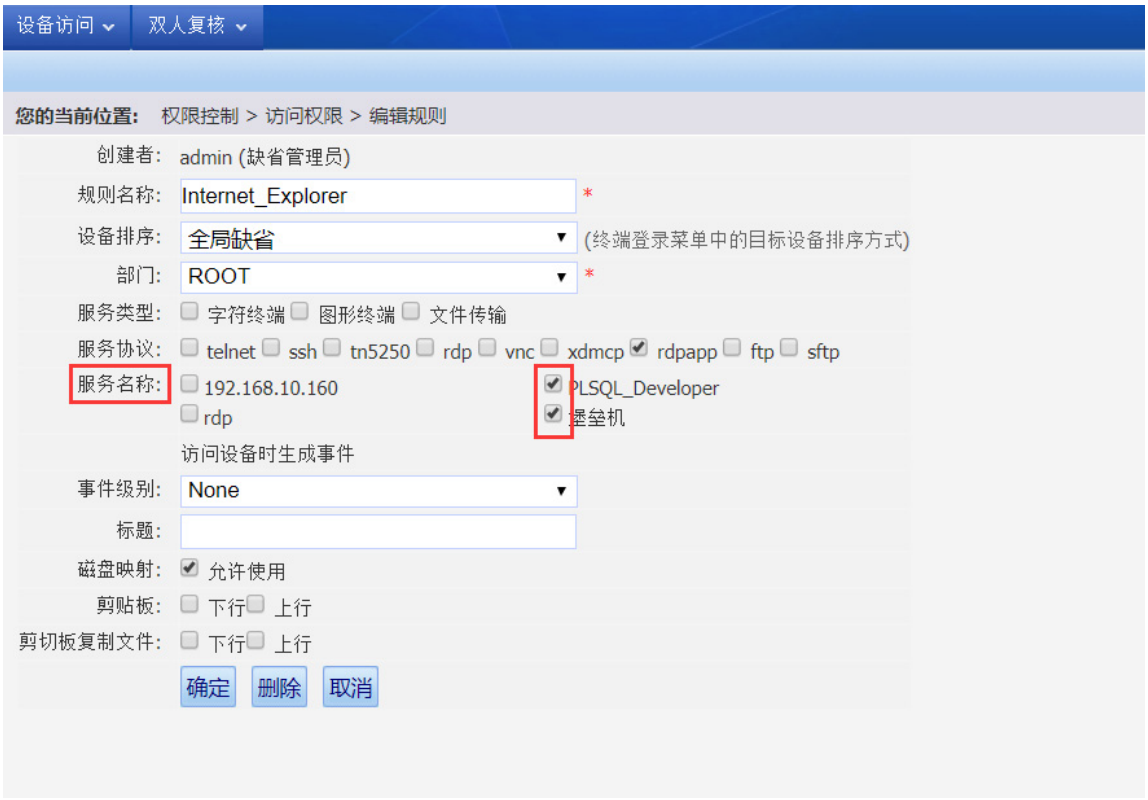
使用配置管理员登录到堡垒机，进入“权限配置”，“权限配置”进行应用访问权限的配置，其中对应的服务协议需选择 rdpapp，如下图所示

图98 应用发布访问权限配置示意图



如果某设备发布了多个应用程序，限制只能使用某个设备中特定应用，可以在访问权限对应的“服务名称”栏进行配置。如下图所示

图99 限制只能使用某个设备中特定应用示意图



4.7 普通用户访问

普通用户先登录堡垒机，然后选择相应的应用程序完成登录，整个过程跟在本地机器上打开应用程序一样。

图100 普通用户访问应用发布器的应用

自动化改密配置举例

目 录

1 简介

自动化改密可以实现对目标设备的系统账号的密码的自动修改、自动备份。

2 配置前提

2.1 选择密码备份方式

密码备份支持邮件服务器发送与文件服务器上传两种方式，选择一种即可。

2.1.1 邮件

(1) 设置 SMTP

使用超级管理员登录，打开[策略配置/系统策略]页面，在系统邮件配置中填写 SMTP 服务器地址与用户名密码。

图1 设置 SMTP

点击<测试>按钮，可以测试邮件是否可以正常发送。

图2 测试

提示

默认情况下运维审计系统使用内置的 SMTP，但是需要正确配置运维审计系统的 DNS 服务器。如果使用其它 SMTP，需提供正确的 SMTP 信息及用户名密码。

(2) 设置密码保管员邮件地址

使用超级管理员登录，打开[基本控制/用户账号]页面，找到密码管理员用户，点击<管理>按钮，添加邮件地址。

图3 设置密码保管员邮件地址

2.1.2 文件服务器

使用超级管理员登录，打开[策略配置/系统策略]页面，在文件服务器配置中的文件服务器 1，协议支持“ftp 或 sftp”，剩余填写服务信息即可。

图4 设置文件服务器

提示

文件服务器中使用的用户需要具有创建目录与创建文件的权限，否则会由于权限错误导致传输失败。

2.2 设置加密密码

使用密码保管员登录，把鼠标移动到右上角账号名字上，在弹出的下拉菜单中选择[账户设置]，输入当前登录密码后点击<确定>按钮，进入账户设置页面。

图5 设置加密密码

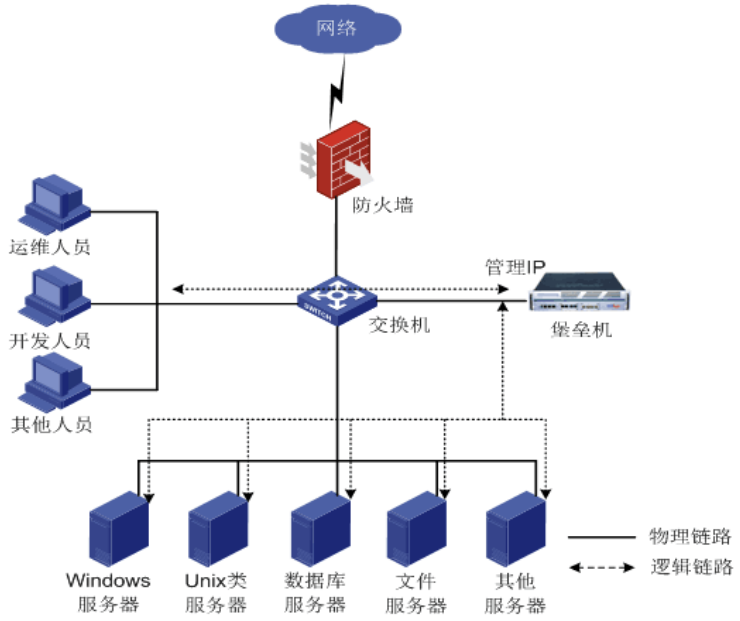
在账户设置页面中，选择<信息交换加密方式>选项卡，在 ZIP 文件密码中输入用于打开保存改密结果的压缩包。

图6 设置加密密码

3 配置举例

3.1 组网需求

图7 运维审计系统组网图



3.2 系统版本要求

适用产品版本：ESS 6102。

3.3 修改Unix/Linux密码

3.3.1 配置思路

- 托管 root 密码，并保证登录测试成功
- 创建改密计划，定期修改设备密码。

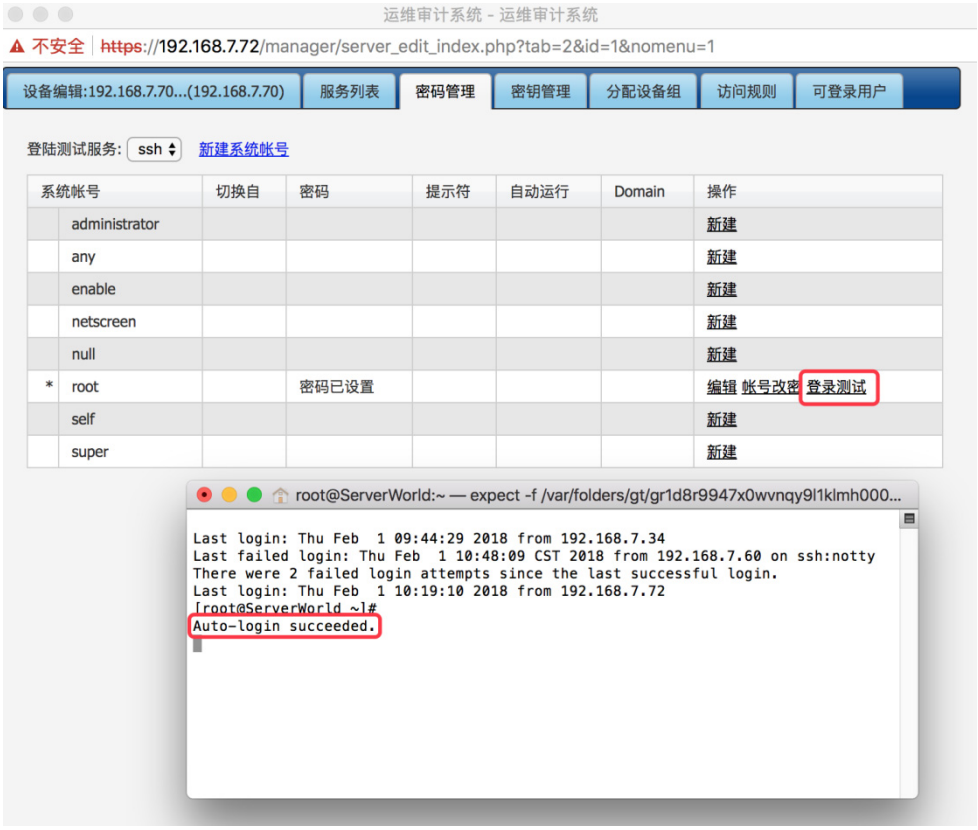
3.3.2 配置步骤

(1) 使用配置管理员登录，打开[基本控制/目标设备]，找到要改密的设备点击<密码管理>按钮。

图8 密码管理

(2) 托管特权账号 root 密码，并可以登录测试成功。

图9 登录测试



(3) 打开[密码控制/改密计划]，点击<新建计划>按钮，创建定期改密计划。

图10 创建定期改密计划

(4) 设置好的改密计划会按照预期时间进行修改，也可以通过手动方式立即执行。

图11 立即执行

提示

只有同时具备配置管理员和密码保管员权限的用户才可以手工设置密码。

3.4 修改Windows密码

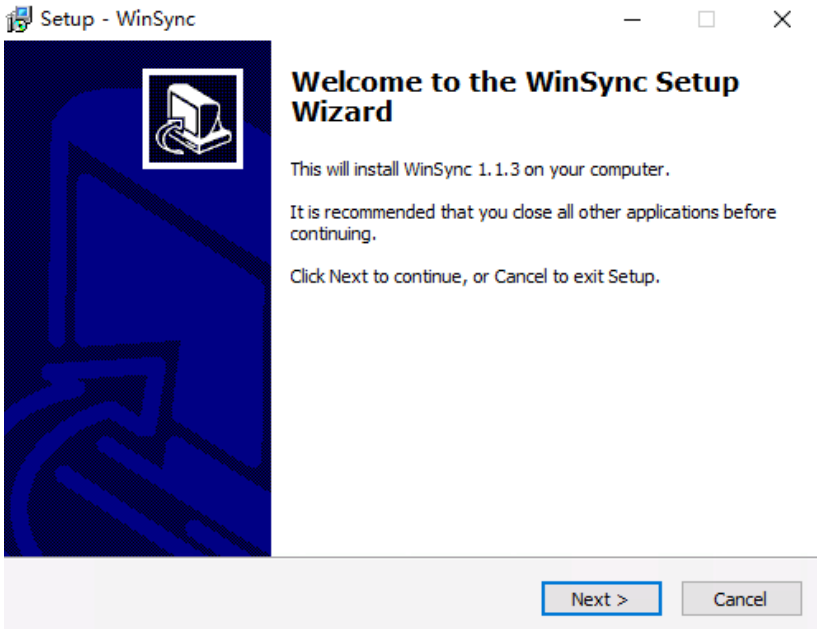
3.4.1 配置思路

- 在目标设备上安装 Winsync 程序。
- 创建改密计划，定期修改设备密码。

3.4.2 配置步骤

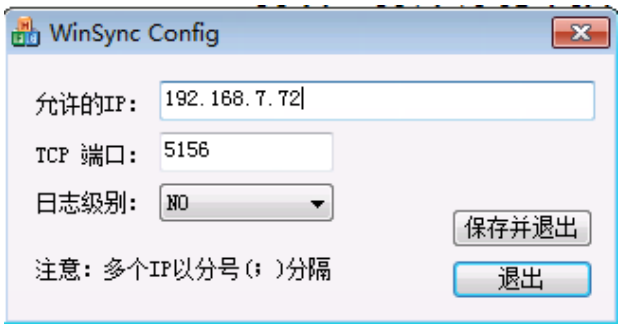
(1) 登录目标设备，安装 winsync 程序，保持默认安装即可。

图12 安装 winsync 程序



(2) 在开始菜单中打开“配置 WinSync”工具，填写允许连接的来源 IP 地址，多个地址时使用分号分隔。

图13 填写登录参数



提示

配置管理员和密码保管员可以在工具下载页面获取 Winsync 工具。

需使用超级管理员权限安装，并确保 SecPath 运维审计系统可以连接目标设备的 5156 端口。

(3) 在开始菜单中点击“重启WinSync”，重启后配置即可生效。若RDP设备改密仍不能与WinSync连接成功，可参考章节 4 1. 进行静默安装WinSync工具。

图14 重启 WinSync

(4) 使用配置管理员登录，打开[基本控制/目标设备]，找到要改密的设备点击<密码管理>按钮。

图15 密码管理

(5) 托管特权账号 administrator 密码，并可以登录测试成功。

图16 登录测试

(6) 打开[密码控制/改密计划]，点击<新建计划>按钮，创建定期改密计划。

图17 创建定期改密计划

(7) 设置好的改密计划会按照预期时间进行修改，也可以通过手动方式立即执行。

图18 立即执行

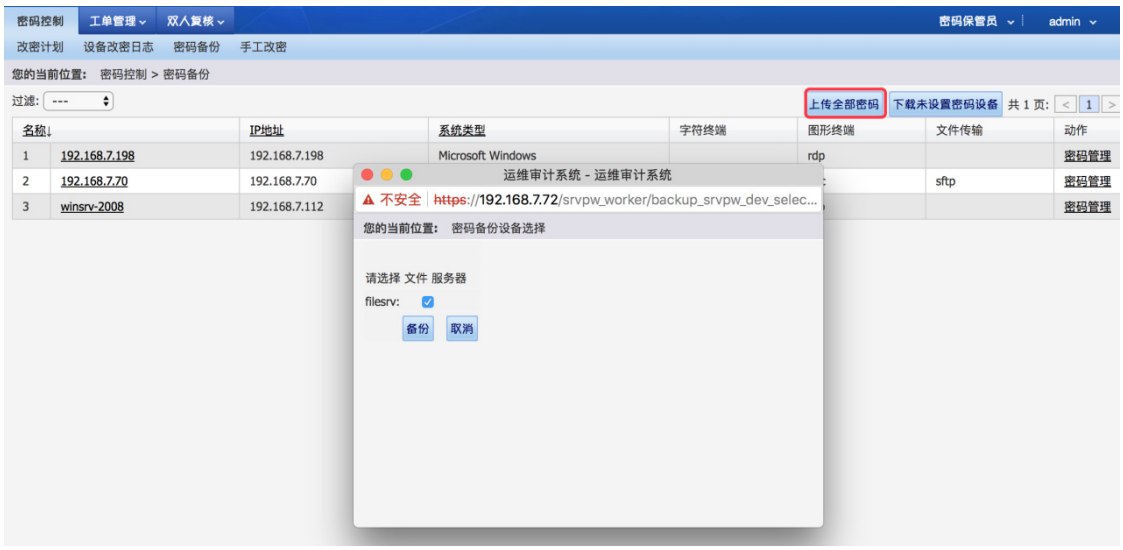
3.5 备份密码到文件服务

(1) 使用超级管理员登录，打开[策略配置/设备密码]，在密码备份规则中勾选“文件服务器”选项。

图19 备份密码到文件服务

(2) 使用密码保管员登录，打开[密码控制/密码备份]，点击<上传全部密码>按钮，在弹出的窗口中选择要上传的服务器即可。

图20 备份密码到文件服务

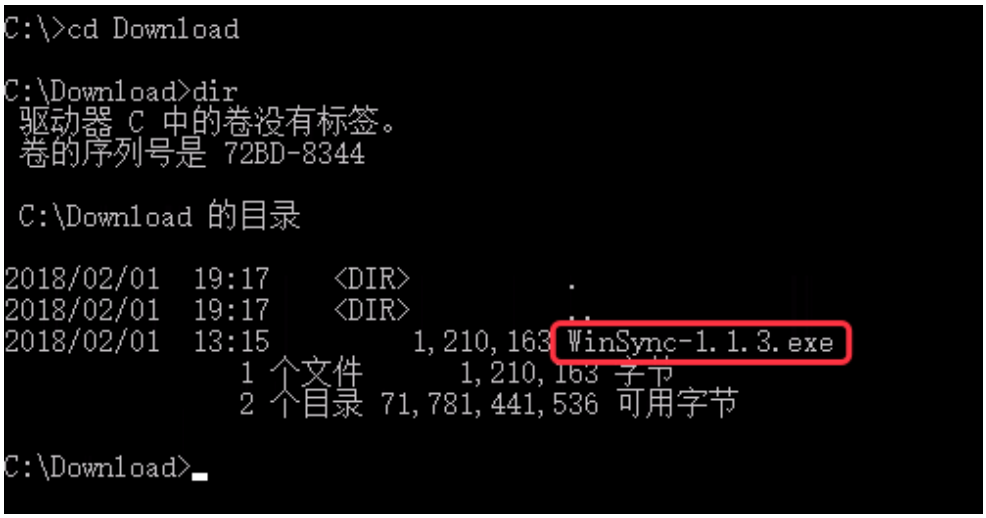


4 常见问题

1. 如何静默安装Winsync工具

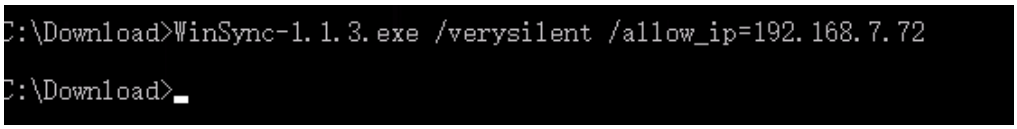
(1) 打开 CMD 工具，进入到 Winsync 存放路径。

图21 进入到 Winsync 存放路径



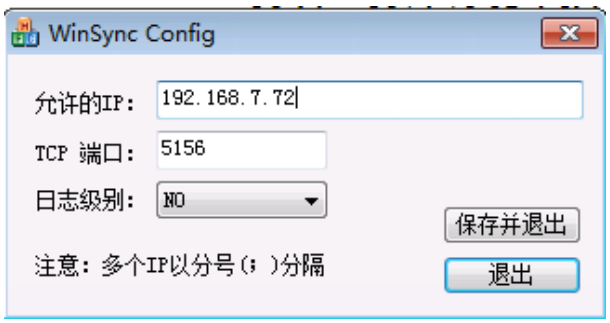
(2) 输入静默安装命令，并指定来源地址。

图22 输入静默安装命令，并指定来源地址



(3) WinSync 静默安装到默认路径，并指定来源地址为 192.168.7.72。

图23 配置登录参数



提示

安装时指定参数 /verysilent 为静默安装，/allow_ip=ip;ip;ip 则可指定允许连接的来源地址，多个地址用分号隔开。
