云翼运维审计系统

用户手册

北京瑞和云图科技有限公司

www.rivercloud.com.cn

2020 年

目录

本书约定……10

前言……11

适用范围和先决条件……11

第一章. 产品简介……12

1.1. 产品概要……12

1.2. 应用场景……13

第二章. 登录云翼运维审计系统……14

2.1. Web 方式登录……14

2.1.1. 密码方式登录……14

2.2. SSH 客户端登录……15

2.2.1. 密码方式登录……15

3.3 找回密码……15

第三章. 仪表盘……16

3.1. 总览……16

3.2. 统计信息……17

3.3. 活跃用户统计……17

3.4. 用户资产排名……18

4.6 待审批工单……18

第四章. 用户管理……19
4.1. 用户列表……19
4.1.1. 用户新建……19
4.1.2. 修改用户信息……20
4.1.3. 删除用户……21
4.1.4. 禁用用户……21
4.1.5. 激活用户……21
4.1.6. 用户详情……22
4.2. 用户组……23
4.2.1. 创建用户组……23
4.2.2. 修改用户组信息……24
4.2.3. 删除用户组……24
4.2.4. 加入用户组……24
第五章. 资产管理……24
5.1. 资产列表……25
5.1.1. 资产管理树……25
5.1.2. 创建资产……27
5.1.3. 更新资产……28
5.1.4. 资产详情……29

5.1.5. 删除资产……29
5.1.6. 禁用资产……30
5.1.7. 激活资产……30
5.1.8. 资产查询……31
5.2. 网域列表……31
5.2.1. 网域列表……32
5.2.2. 创建网域……32
5.2.3. 更新网域……32
5.2.4. 网关列表……33
5.2.5. 创建网关……33
5.2.6. 更新网关……34
5.2.7. 测试连接……34
5.3. 管理用户……35
5.3.1. 管理用户列表……35
5.3.2. 创建管理用户……36
5.3.3. 更新管理用户……36
5.3.4. 删除管理用户……36
5.3.5. 查询管理用户……37
5.3.6. 管理用户导入……37

5.3.7. 管理用户导出……38

5.3.8. 批量更新……39

5.4. 系统用户……39

5.4.1. 系统用户列表……40

5.4.2. 创建系统用户……40

5.4.3. 系统用户详情……41

5.4.4. 更新系统用户……42

5.4.5. 删除系统用户……42

5.4.6. 查询系统用户……43

5.4.7. 系统用户导入……43

5.4.8. 系统用户导出……44

5.4.9. 批量更新……44

5.5. 标签管理……45

5.5.1. 创建标签……45

5.5.2. 更新标签……45

5.5.3. 删除标签……46

5.5.4. 查询标签……46

5.6. 命令过滤……46

5.6.1. 命令过滤列表……47

5.6.2. 创建命令过滤器……47
5.6.3. 规则查询……48
5.7. 平台列表……49
第六章. 应用管理……50
6.1. 数据库应用……50
6.2. 新建数据库应用……50
第七章. 应用发布……53
7.1. 应用发布……53
7.2. 应用发布搭建方案……53
7.2.1 安装远程桌面服务……58
7.2.2 安装 RemoteApp 服务……71
7.2.3 远程授权桌面……81
7.2.4 调整本地组策略……108
7.2.5 关闭 Windows 防火墙……117
7.2.6 关闭 IE 增强的安全配置……118
7.2.7 添加 RD 授权……121
7.2.8 设置 RD 授权模式……123
7.2.9 开启远程桌面……128
7.2.10 发布 RemoteApp 程序……131

7.3. 如何生成应用……139

7.4. 应用发布使用方法……142

7.5. 应用分配功能……144

第八章. 权限管理……146

7.6. 资产授权……146

7.1.1. 查看授权列表……146

7.1.2. 创建授权规则……146

7.1.3. 更新授权规则……147

7.1.4. 删除授权规则……148

7.1.5. 查询授权规则……148

7.7. 数据库应用……148

7.2.1. 数据库应用规则列表……149

7.2.2. 创建数据库应用规则……149

7.2.3. 更新数据库应用规则……149

7.2.4. 删除数据库应用规则……150

7.2.5. 查询数据库应用规则……150

第九章. 会话管理……151

8.1. 在线会话……151

8.1.1. 查看在线会话……151

8.1.2. 中断在线会话……152
8.2. 历史会话……153
8.2.1. 历史会话列表……153
8.3. 命令记录……153
8.4. Web 终端……154
8.5. 文件管理……155
8.6. 终端管理……157
8.6.1. 存储配置……157
第十章. 作业中心……159
9.1. 任务列表……159
9.2. 批量命令……160
9.3. 任务监控……160
第十一章. 日志审计……161
10.1. 登录日志……161
10.1.1. 日志查询……161
10.1.2. 日志导出……162
10.2. FTP 日志（无数据）……162
10.2.1. FTP 日志查询……162
10.3. 操作日志……163

10.4. 改密日志……163

10.5. 批量命令……164

10.5.1. 批量命令执行详情……164

第十二章. 系统设置……164

11.1. 基本设置……164

11.2. 邮件设置……165

11.3. LDAP 设置……165

11.4. 终端设置……166

11.5. 安全设置……167

11.6. Syslog 日志设置……167

本书约定

1、 鼠标操作约定

操作	意义
单击	快速按下并释放鼠标的一个按钮。
双击	连续两次快速按下并释放鼠标的一个按钮。
拖动	按住鼠标的一个按钮不放，移动鼠标。

2、 各类标志

本书还采用各种醒目的标志来表示需要特别注意的地方，这些标志的含义如下： 注意：提醒应该注意的事项。

说明：对内容进行必要的补充和说明。

前言

适用范围和先决条件

旨在为 IT 审计员、IT 顾问和安全专家提供可靠的服务器和应用发布管理安全解决方案，帮助 IT 决策者应对各类法令法规（如 SOX、PCI、企业内控管理、等级保护、ISO/IEC27001 等），同时帮助 IT 运维人员更高效地执行自动化运维和资源监控操作。本手册编写以帮助用户了解系统使用、根据使用场景构建出属于自己的云计算安全管控系统。

要成为一个合格的运维审计系统管理员，必须具备以下技能：

- 基本的系统管理（Windows、Linux、Unix 以及各类网络设备）知识
- 熟悉计算机网络、TCP/IP 协议以及常用网络术语

第一章. 产品简介

1.1. 产品概要

云翼运维审计系统（简称堡垒机）是用于提供信息系统安全管控的系统和组件，实现对运维资源的 4A 全面安全管控。系统包含用户管理、资源管理、策略、审计、工单等模块，支持对 Windows 主机、Linux 主机等诸多主机的安全管控保护。是集统一资产管理与单点登录，多种终端访问协议，文件传输功能于一体的运维安全管理与审计产品，产品特色及优势主要体现以下几个方面：

- 无需客户端，在登录资源，或对其实时监控和上传下载文件时无需安装任何客户端软件。
- 集中账号管理，统一维护主机、网络设备和应用发布等资源。记录与审计，支持访问历史记录回放和操作指令搜索功能，可随时查看每个用户对所属主机、主机和网络设备的访问情况。
- 细粒度的权限划分及对用户的动态授权功能。
- 敏感命令拦截，对云翼运维审计系统所管控的主机进行实时命令拦截。

云翼运维审计系统为政府部门、电信运营商、金融机构、企事业单位、商业组织等提供了完整的统一安全管理平台解决方案，使客户在面对高复杂度的内控授权、运维操作审计、法律法规合规性审查时，能够实施完善的解决方案。

部署运维审计系统，能够极大的保护客户内部网络设备及主机资源的安全性，提高运维效率,使得客户的网络管理更加统一、安全和便捷。

1.2. 应用场景

满足政策、法规需求：运维审计系统能满足各类法令法规（如 SOX、PCI、企业内控管理、等级保护、ISO/IEC27001 等）对运维审计的要求。能够细粒度地划分不同角色的权限，达到控制管理员对服务器的访问，并且提供大数据智能审计功能，对所有运维操作能达到很好的审计、监控、控制和历史回放效果。

管理外部 IT 运维人员：许多公司聘请了外部 IT 运维人员来进行各类主机和设备的配置、维护和管理，这些主机中可能包含着重要的邮件、客户信息和关键业务服务，这种行为实际上意味着公司需要绝对信任外部 IT 运维人员。在这种情况下，拥有可靠的外部设备来监控、审计

运维操作就显得至关重要。部署运维审计管理系统后，既能满足对 IT 运维人员所有操作的记录和回放，又能实时监控与阻断在线 IT 运维人员，达到对外部 IT 运维人员操作的全监控。

远程管理的控制：许多公司都拥有需要在互联网上远程管理的主机和设备，部署运维审计系统，更好的强化对主机或设备的安全管理，追踪每次运维操作的具体细节。

SSH、TELNET、RDP、VNC、SFTP、FTP 协议控制：云翼运维审计系统能对 SSH、TELNET 等字符控制协议提供支持，利用自身技术优势，无论对加密协议（如 SSH、RDP、SFTP）或非加密协议（如 TELNET、VNC、FTP）都能实现完全的监控和事后审计。让用户对支持不同协议的设备监控和审计操作更加简单和易用。

第二章. 登录云翼运维审计系统

2.1. Web 方式登录

2.1.1. 密码方式登录

云翼运维审计系统基于 Web 界面登录的方式，支持各种主流浏览器: IE10 浏览器及以上版本，Chrome 浏览器，Firefox 浏览器，Safari 浏览器等。

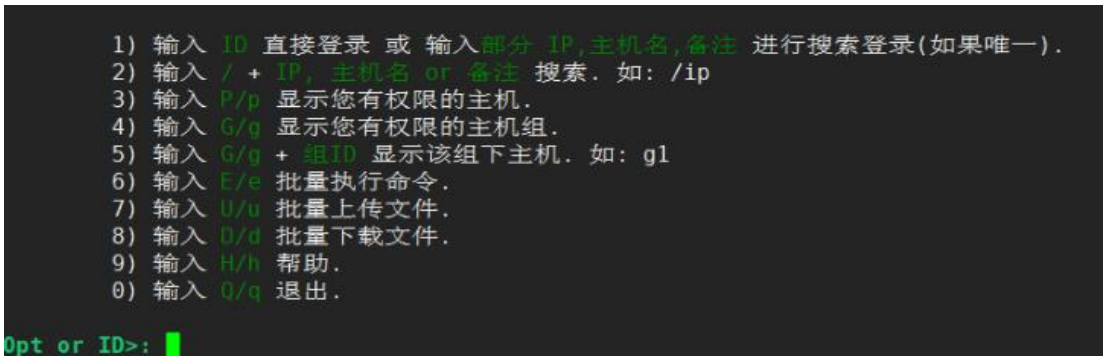
请首先启动浏览器，并且输入云翼运维审计系统的 IP 地址和端口（例如 http://192.168.0.254）到地址栏，然后按下<Enter>键，进入登录界面；如图 I 所示。输入“admin”（云翼运维审计系统默认系统管理员账号）到用户名输入栏里，输入密码，最后单击<登录>按钮。

图 I.

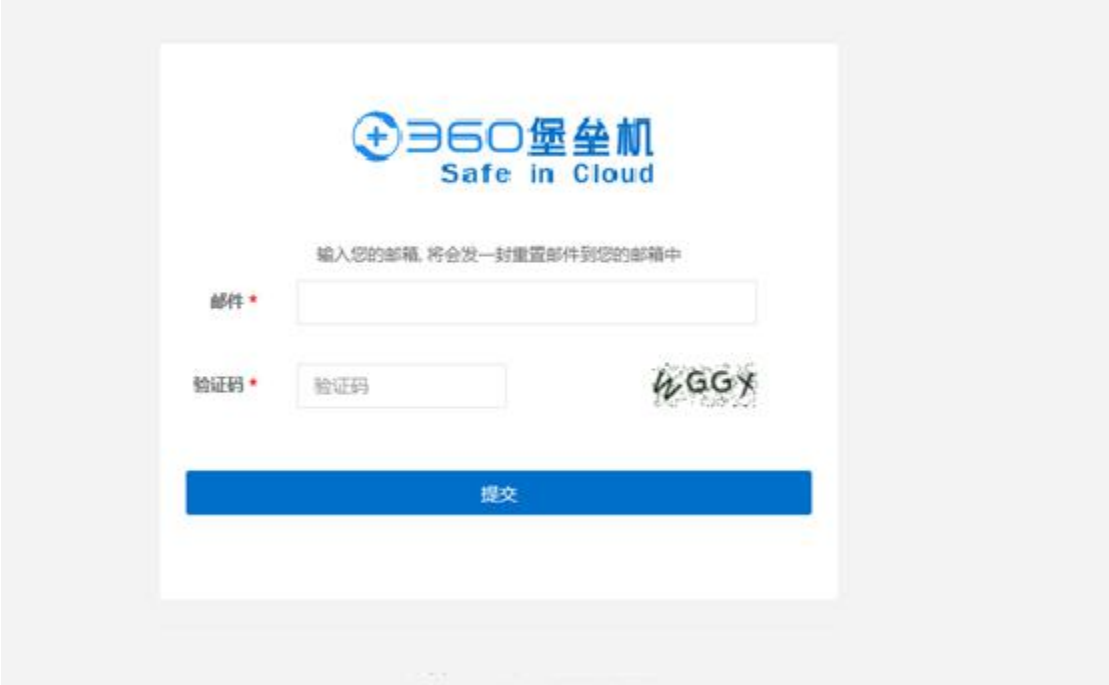
2.2. SSH 客户端登录

2.2.1. 密码方式登录

云翼运维审计系统也可以使用 SSH 客户端登录的方式，打开 SSH 客户端（比如 Xshell），新建一个会话， 在主机栏中输入云翼运维审计系统的 IP 地址（例如 192.168.0.254），在端口号栏中填写默认的端口号 2222， 然后点击<确定>按钮，选择刚刚新建的会话，点击<连接>按钮或是双击刚刚新建的会话，进入登录界面；输入用户名，点击<确定>按钮，并输入密码点击<确定>按钮即可登录成功，如下图 所示。



3.3 找回密码



系统管理员创建用户或是用户自行登录系统后，如果填写过正确邮箱，在之后的使用过程中用户如果忘记系统登录密码，可以通过登录首页的找回密码功能对密码进行重置。点击登录页面的<忘记密码?>，填写邮件地址，如上图所示，填写正确信息后，进入邮箱点解密码重置邮件中的链接，完成密码重置。

第三章. 仪表盘

下面以系统管理员为例讲解其登录后仪表盘的各项含义。

3.1.总览

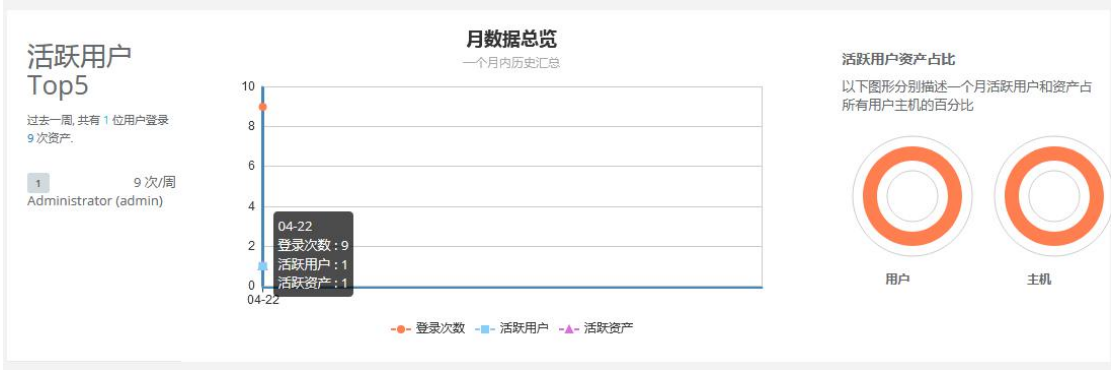
进入[仪表盘]，将会看到正在管理的资产和用户活动状态如下图所示。

3.2.统计信息

统计云翼运维审计系统当前用户总数、主机总数、当前在线用户和在线主机数。点击数字可以跳转到相应的管理界面。

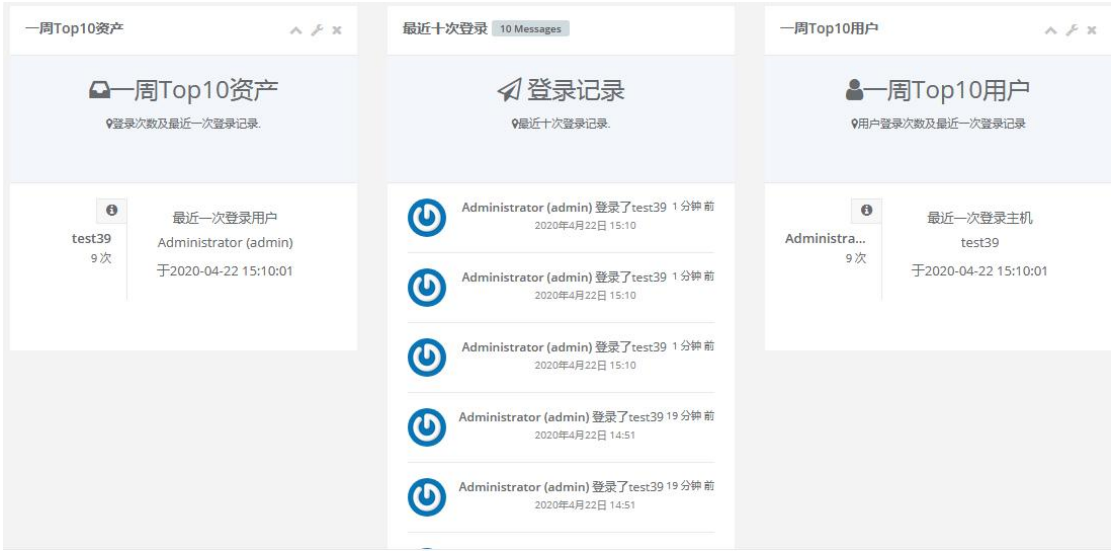
3.3.活跃用户统计

统计云翼运维审计系统活跃用户排名、月数据总览以及用户登录主机统计。鼠标放置在图中会有详细数据展示。



3.4.用户资产排名

统计云翼运维审计系统登录的用户和资产排名情况统计。



4.6 待审批工单

进入[桌面]，查看[待审批工单]控制板，可显示用户角色权限范围内的待审批工单，点击可跳转工单详情。该控制板是否显示由用户角色是否拥有工单审批模块权限和管理权限决定，如图 4-6-1、4-6-2 所示。

第四章. 用户管理

4.1. 用户列表

4.1.1. 用户新建

进入[用户/用户列表]，点击页面左上方的<创建用户>按钮，进入新建用户页面，如下图所示。

进入[创建用户]界面，编辑用户信息，其中“*”标记的红色部分为必填项。其中需要注意的是新密码和确认密码的填写需要保存一致；用户名即云翼运维审计系统登录账号。用户是用于资产授权,当某个资产对一个用户授权后,这个用户就使用这个资产了。角色用于区分一个用户是管理员还是普通用户。点击<生成重置密码链接，通过邮件发送给用户>，可以通过邮件发送更改密码的链接。填写好所有必填项信息后，点击<提交>按键完成创建。

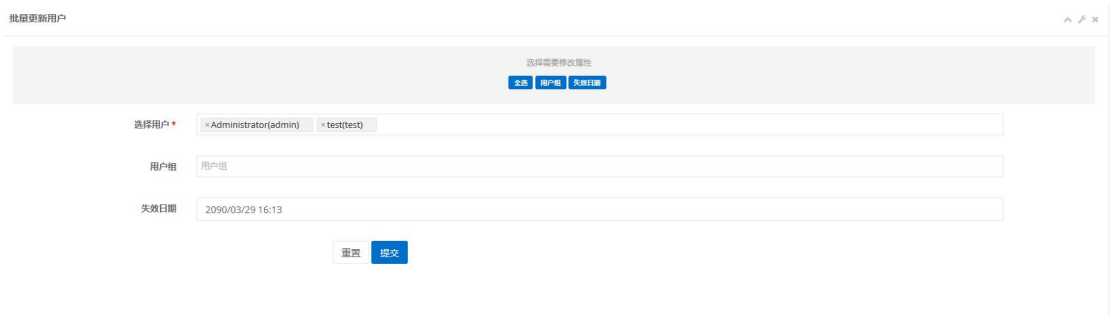
成功提交用户信息后，云翼运维审计系统会发送一条设置"用户密码"的邮件到您填写的用户邮箱。

点击邮件中的设置密码链接，设置好密码后，您就可以用户名和密码登录 云翼运维审计系统了。

4.1.2. 修改用户信息

进入[用户/用户列表]，点击用户列表右边的<更新>按钮，进入修改用户页面，可修改用户信息。

在用户列表中，同时勾选多个用户，然后选择列表下方的<批量更新>，可以一次性更新多个用户的用户组以及失效日期，如下图：



4.1.3. 删除用户

选择一条用户信息，点击最右侧的<删除>，点击<确认>可删除该用户信息。

在用户列表中，同时勾选多个用户，然后选择列表下方的<批量删除>，可以一次性删除多个用户。

4.1.4. 禁用用户

在用户列表中，同时勾选一个或多个用户，然后选择列表下方的<禁用所选>，可以一次性禁用一个或多个用户。

4.1.5. 激活用户

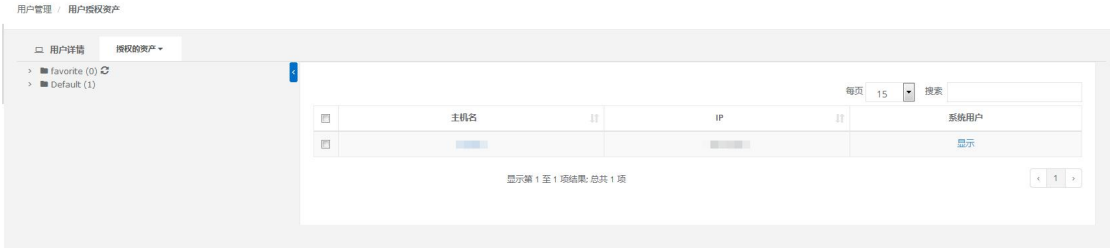
在用户列表中，同时勾选一个或多个用户，然后选择列表下方的<激活所选>，可以一次性激活一个或多个用户。

4.1.6. 用户详情

在[用户列表]页面，点击对应用户名称可看到改用的详情以及授权的资产。

在此页面用户也可以对以下功能进行操作。

在<授权的资产>标签页，可以查看该用户被授权了哪些资产，点击资产名称可以直接跳转至<资产详情>页。



点击资产对应的显示，可以显示该资产所使用的系统用户。

4.2. 用户组

4.2.1. 创建用户组

用户组可以将云翼运维审计系统的用户进行分组。通常在分配资产权限的时候，针对的某个用户组下的所有用户，可以为一个用户分配多个用户组。点击页面左侧"用户管理"菜单下的"用户组"，进入用户组列表页面。

点击页面左上角"创建用户组"按钮，进入创建用户组页面：

名称即用户组名称，建议填写简单明了有用的信息。创建用户组的时候可以把已存在的用户加入到该分组中，一个用户可以存在多个分组中。

4.2.2. 修改用户组信息

选择一条用户组，点击右侧的<更新>进入编辑页面，可对用户组信息进行修改，编辑完成后点击<确认>。

4.2.3. 删除用户组

选择一条用户组，点击最右侧的<删除>，点击<确认>可删除该用户信息。

4.2.4. 加入用户组

进入[用户管理]，点击指定用户对应操作中的<更新>按键，可以将用户加入或者移除组。

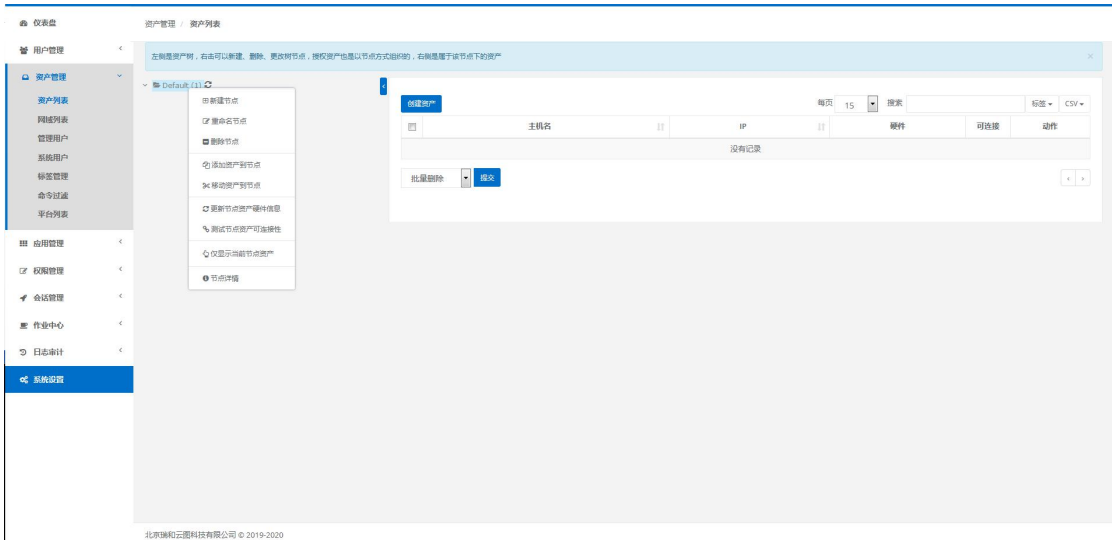
第五章. 资产管理

资产管理可对 Windows 和 Linux 主机以及网络设备进行管理。

5.1.资产列表

5.1.1. 资产管理树

资产树节点不能重名，右击节点可以添加、删除和重命名节点，以及进行资产相关的操作。



1、 节点管理

为了方便的对资产进行分组管理，用户可以在此对不同资产的分组进行新建、编辑、删除等操作。

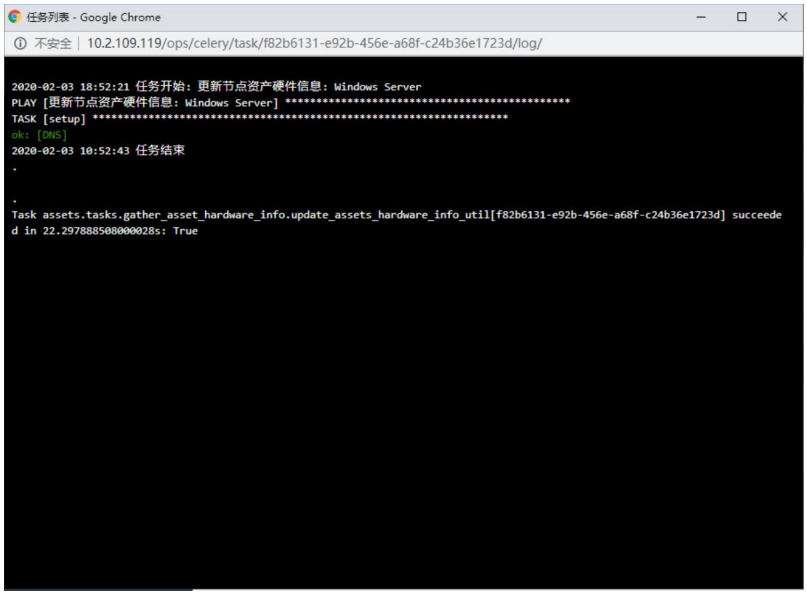
2、 添加和移动资产到节点

如果在新添加资产时没有指定节点，或者新建节点后需要将资产添加或移动至该节点，则需要使用此操作。

选中要添加到该节点的资产，点击<确认>。

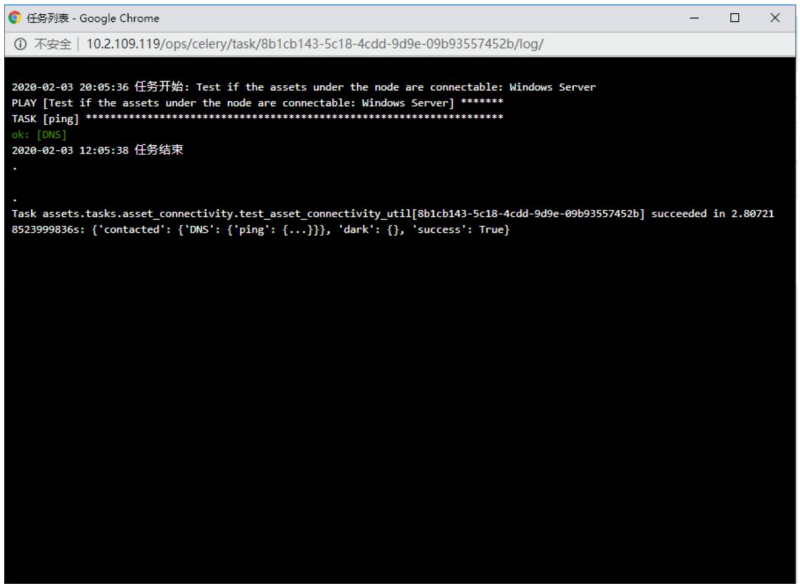
3、 更新节点资产硬件信息

在某个资产树下面的资产硬件出现变动的时候，执行更新节点资产硬件信息可以将资产的硬件变动同步至云翼运维审计系统中，方便管理员进行资产核查。在左侧资产树中的右键菜单中选择<更新节点资产硬件信息>，在弹出的任务执行窗口中显示如下图所示时，表示资产更新已经完成。



4、 测试节点资产可连接性

当添加新的资产后，可在此测试节点的可连接性。



5.1.2. 创建资产

在资产列表页面，先在左侧选择资产要加入的节点，然后在右侧选择创建资产。首先填写主机基本信息，输入主机参数，其中“*”标记的红色部分为必填项，“主机名”允许填写中文、数字、英文字母等，“系统平台”可选 Linux、Unix、MacOS、BSD、Windows、Windows（2016）、Other，“协议组”可选 SSH、RDP、VNC、TELNET，“主机 IP”填写需要被云云翼运维审计系统管控的主机 IP 地址，“端口” 根据所选主机类型可自动填写，也可修改。其余为非必填项。

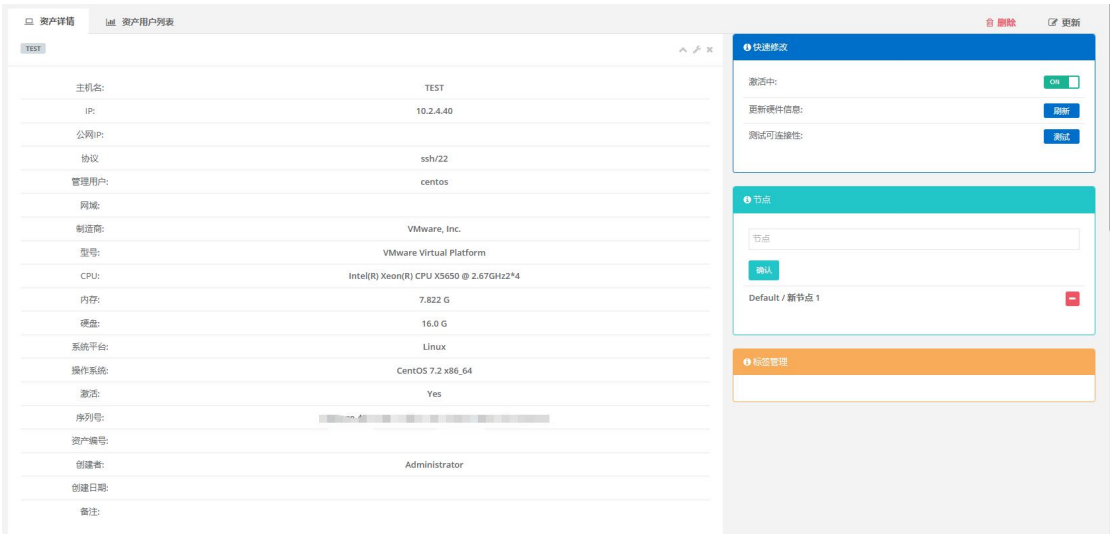
5.1.3. 更新资产

如果被管理的资产信息发生了变化，如 IP 改变、用户更新等等，则需要在云翼运维审计系统上对相应的资产做更新处理。

支持批量更新主机，勾选需要更新的主机，点击下方的<批量更新>按钮，如图所示。

5.1.4. 资产详情

进入[资产列表]，点击主机名称进入详情页面，可以查看到主机的基本信息、资源账户信息和授权用户。



5.1.5. 删除资产

进入[资产列表]，选择指定机器，点击<删除>按钮，如图所示。

支持批量删除主机，勾选需要删除的主机，点击下方的<批量删除>按钮，如图所示。

5.1.6. 禁用资产

在资产列表中，同时勾选一个或多个资产，然后选择列表下方的<禁用所选>，可以一次性禁用一个或多个资产。

5.1.7. 激活资产

在资产列表中，同时勾选一个或多个资产，然后选择列表下方的<激活所选>，可以一次性激活一个或多个资产。

5.1.8. 资产查询

进入[资产列表]，在输入框内输入关键词（支持搜索主机名称、主机地址），点击查询结果，如图所示。

也可以按照标签分类来查询资产，进入[资产列表]，点击在搜索框右侧的<标签>，选择目标标签，如图所示：

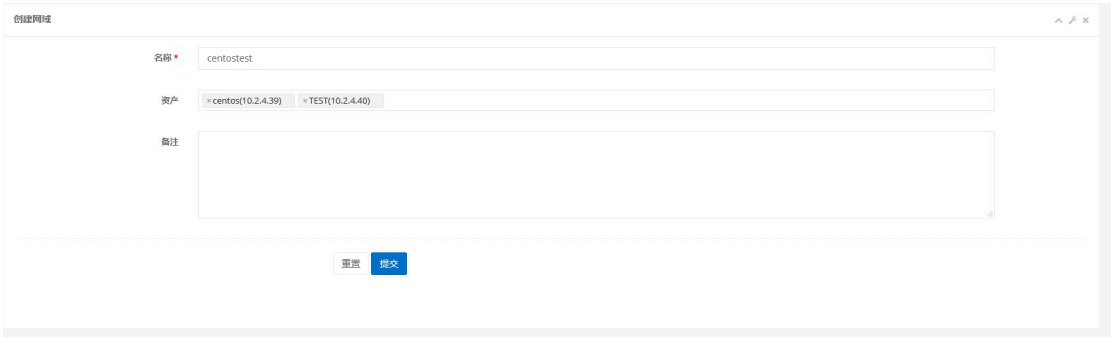
5.2.网域列表

网域功能是在多云环境下使用的，其原理是通过多云环境中的网关服务器进行跳转登录。

5.2.1. 网域列表

5.2.2. 创建网域

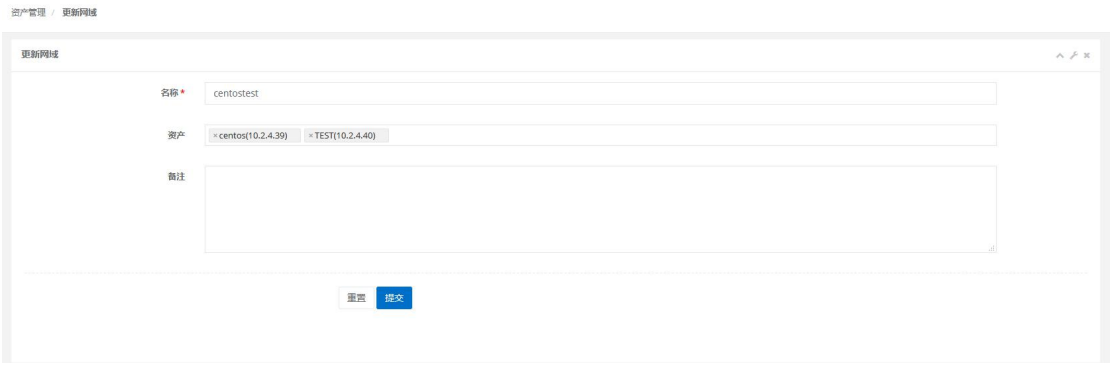
在[网域列表]页面，在右侧选择<创建网域>



5.2.3. 更新网域

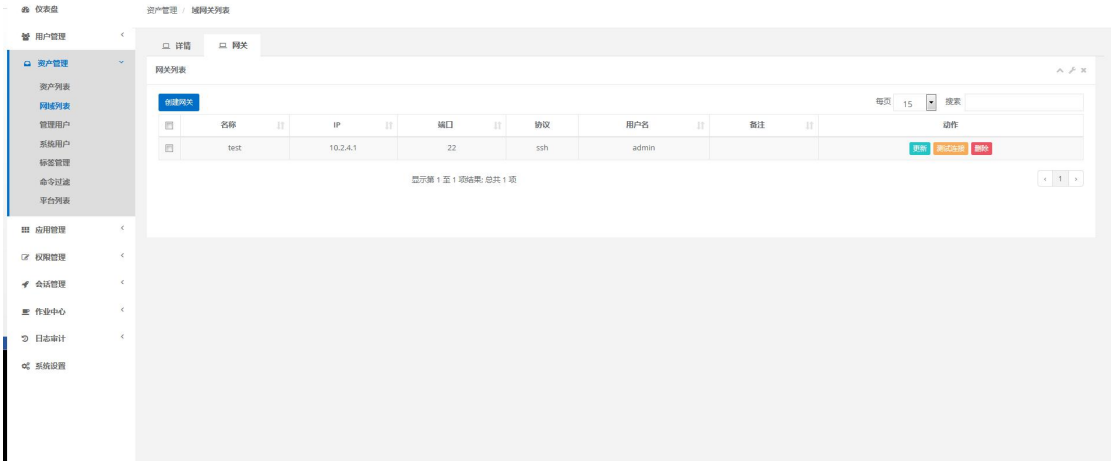
更新网域有两种方式：1、在网域列表处点击需要更新信息的网域右边的更新按钮。2、点击网域名称。

点击网域名称后，点击右侧的<更新>，即可跳转至更新页面。



5.2.4. 网关列表

点击网域名称，可以进入网域详情页面，详情页的右侧是该网域的网关列表页。



5.2.5. 创建网关

在网域列表页面，点击网关下面的数字进入网关列表，点击创建网关，网关可以是一台任意装有 ssh 服务的资产

5.2.6. 更新网关

导航至网关页面，点击需要更新的网关对应的<更新>按钮，修改完信息后，点击<提交>。同样，在此页面可以对失效的网关进行删除操作。

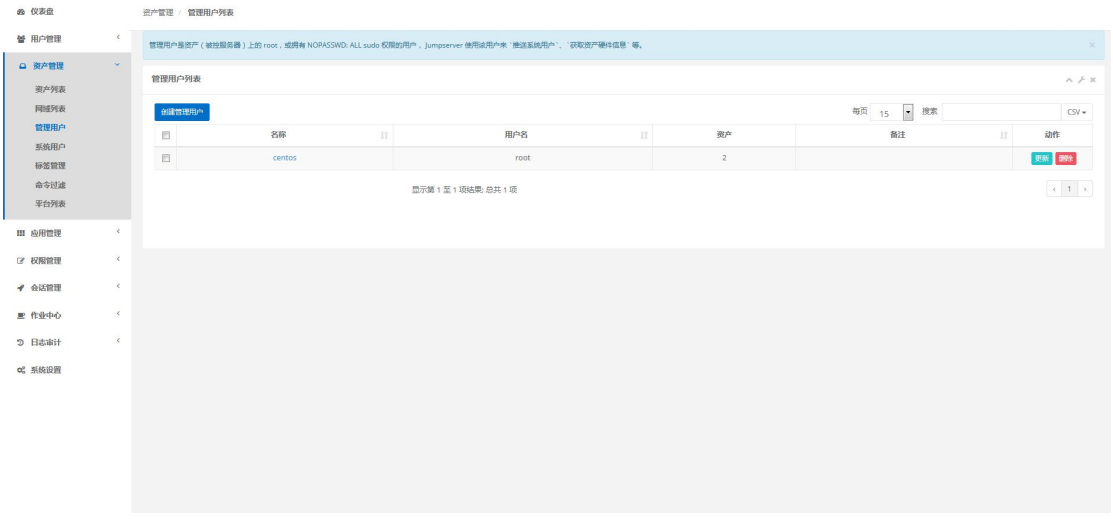
5.2.7. 测试连接

添加完网关之后，可以测试其连通性，点击右侧的<测试连接>按钮即可测试。

5.3.管理用户

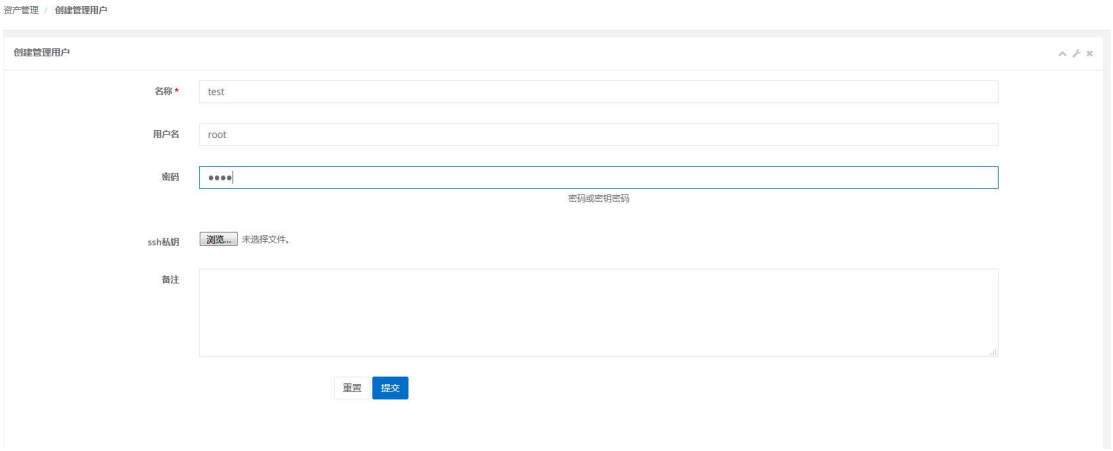
在 Linux 系统中，管理用户是资产 (被控服务器) 上的 root，或拥有 NOPASSWD: ALL sudo 权限的用户，云翼运维审计系统使用该用户来推送系统用户、获取资产硬件信息等。Windows 系统请填写 administrators 组里面的用户。

5.3.1. 管理用户列表



5.3.2. 创建管理用户

点击创建<管理用户>按钮，在新建页面填入正确信息，点击<提交>。



5.3.3. 更新管理用户

找到需要操作的管理用户，点击右侧对应的<更新>按钮。

5.3.4. 删除管理用户

进入[管理用户]界面，点击指定账户的<删除>按钮，删除指定的账户。

5.3.5. 查询管理用户

进入[管理用户]，在搜索输入框内容输入用户名关键词，列表会自动显示符合条件的用户，如图。

5.3.6. 管理用户导入

进入[管理用户]，点击<CSV>，选择导入，如图所示。

注意：

1. 文件导入目前支持导入只能上传 CSV 文件。
2. 导入的用户名称不能与现有的重复。

5.3.7. 管理用户导出

进入[管理用户]，点击<CSV>，选择导出，如图所示。

注意：

1. 如果未选中任何账户，点击【导出】，则导出当前筛选的全部账户
2. 如有选中账户，点击【导出】，则导出选中账户

5.3.8. 批量更新

进入[管理用户]，点击<CSV>，选择更新，如图所示。

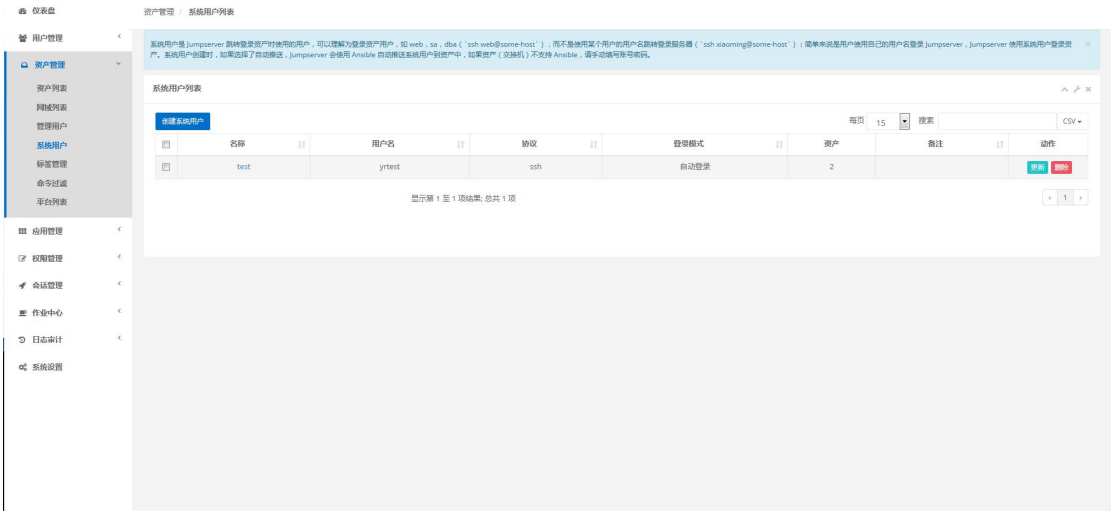
注意：

1. 不要更改用户的 ID。

5.4.系统用户

系统用户是云翼运维审计系统跳转登录资产时使用的用户，可以理解为登录资产用户，如 web, sa, dba(ssh web@some-host)，而不是使用某个用户的用户名跳转登录服务器(ssh xiaoming@some-host)；简单来说是用户使用自己的用户名（xiaoming）登录云翼运维审计系统，云翼运维审计系统使用系统用户登录资产。系统用户创建时，如果选择了自动推送云翼运维审计系统会使用 ansible 自动推送系统用户到资产中，如果资产不支持 ansible，请手动填写账号密码（域用户格式: user@domain.com）。

5.4.1. 系统用户列表



5.4.2. 创建系统用户

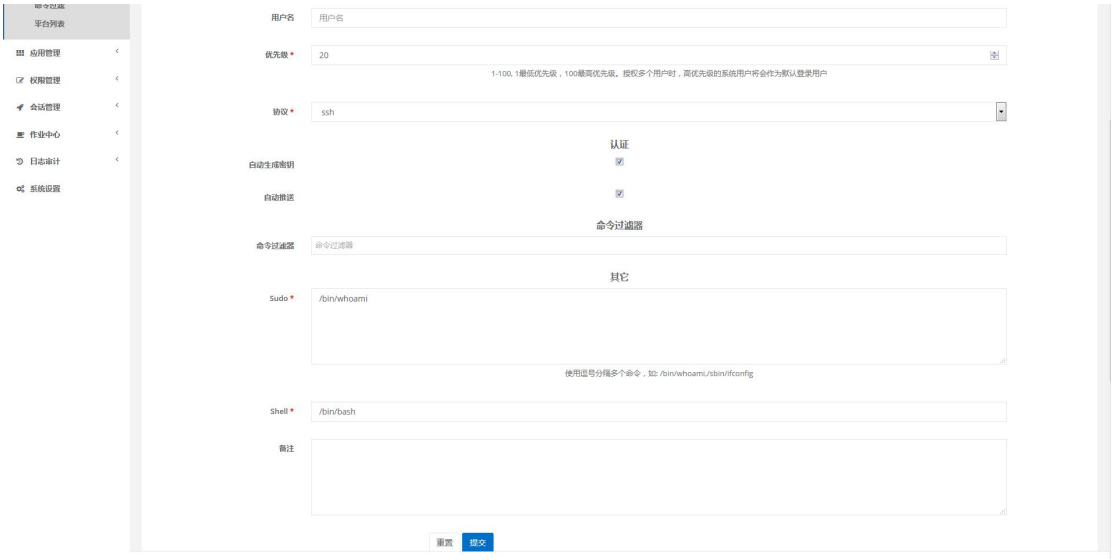
在[系统用户]界面，点击<创建系统用户>按钮，进入创建系统用户界面。

用户主要有以下几种类型：

1. 自动登录用户:用户、密码必填
2. 手动登录用户:用户非必填，密码输入框禁用

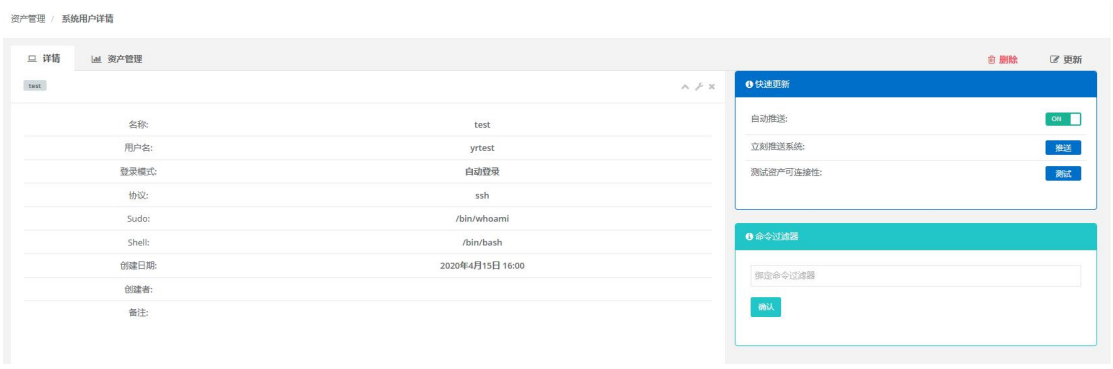
协议主要有以下几种类型：

1. ssh:Linux 类操作系统使用的远程连接协议
2. rdp:Windows 类操作系统所使用的远程连接协议
3. telnet:网络设备操作系统所使用的远程连接协议
4. vnc:Linux 类操作系统使用的图形化远程连接协议
5. mysql:云翼运维审计系统用于连接 MySQL 数据库的连接协议



5.4.3. 系统用户详情

进入[系统用户]，点击名称进入详情页面，可以查看到账户的基本信息和授权资产。



5.4.4. 更新系统用户

进入[系统用户]，点击<更新>，修改账户基本信息，如图

5.4.5. 删除系统用户

进入[系统用户]，点击指定账户的<删除>按钮，删除指定的账户。

5.4.6. 查询系统用户

进入[系统用户]，在搜索输入框内容输入用户名关键词，列表会自动显示符合条件的用户，如图。

5.4.7. 系统用户导入

进入[系统用户]，点击<CSV>，选择导入，如图所示。

注意：

1. 文件导入目前支持导入只能上传 CSV 文件。
2. 导入的用户名称不能与现有的重复。

5.4.8. 系统用户导出

进入[系统用户]，点击<CSV>，选择导出，如图所示。

注意：

1. 如果未选中任何账户，点击【导出】，则导出当前筛选的全部账户
2. 如有选中账户，点击【导出】，则导出选中账户

5.4.9. 批量更新

进入[系统用户]，点击<CSV>，选择更新，如图所示。

注意：

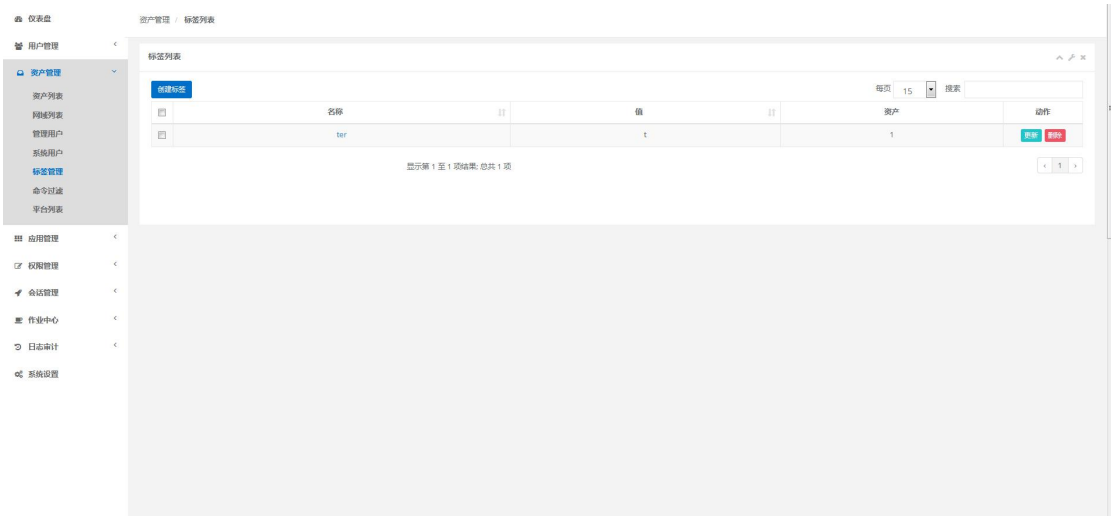
1. 不要更改用户的 ID。

5.5.标签管理

给资产打上标签便于查询和管理。标签信息有名称和值：名称可以是描述功能信息，例如：用途，值则可以是具体信息，例如：组织 1-部门 1-研发。标签创建的时候可以选择为已存在的资产打上该标签。标签名称可以重名，一个资产可以有多个标签产。标签删除，资产上的标签信息会自动消失。

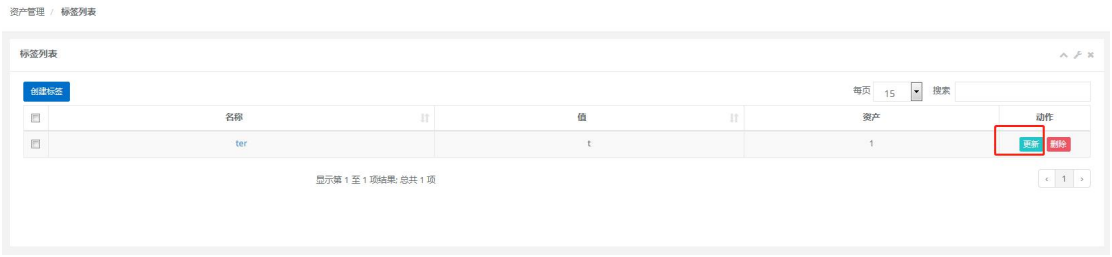
5.5.1. 创建标签

进入[标签管理]列表，通过点击<创建标签>按钮，可以为资产创建标签，如图所示。



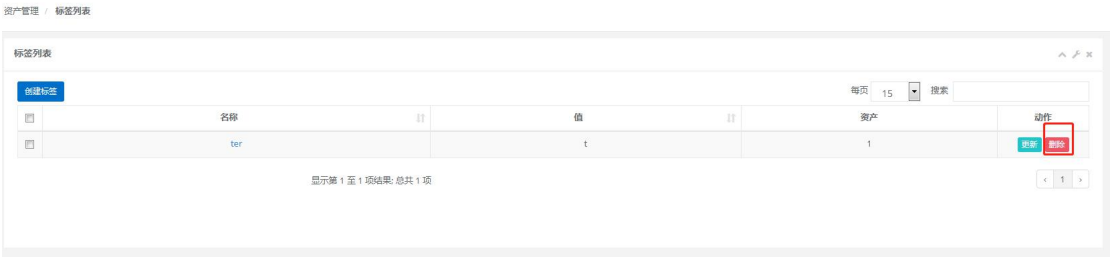
5.5.2. 更新标签

进入[标签管理]列表，通过点击<更新>按钮，可以为资产更新标签，如图所示。



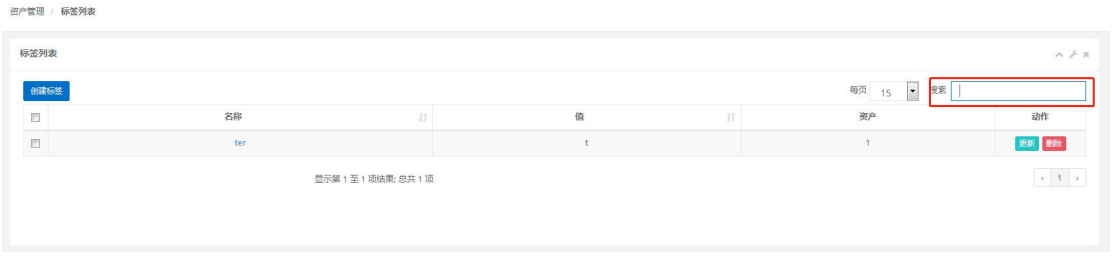
5.5.3. 删除标签

进入[标签管理]列表，通过点击<删除>按钮，可以删除标签，如图所示。



5.5.4. 查询标签

进入[标签管理]，在搜索输入框内容输入关键词（可以是名称或值），列表会自动显示符合条件的标签，如图。

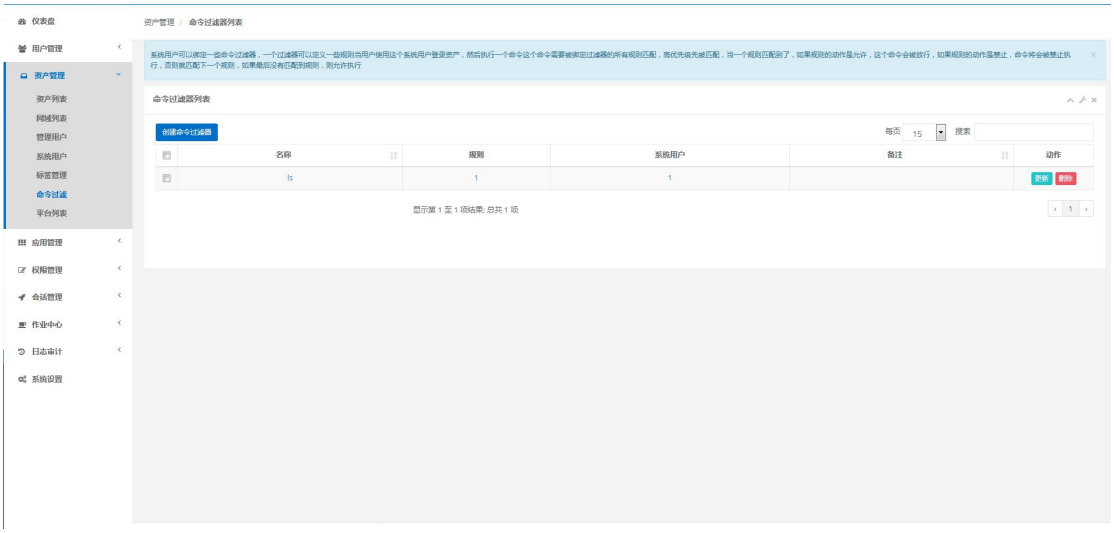


5.6.命令过滤

系统用户可以绑定一些命令过滤器，一个过滤器可以定义一些规则。当用户使用这个系统用

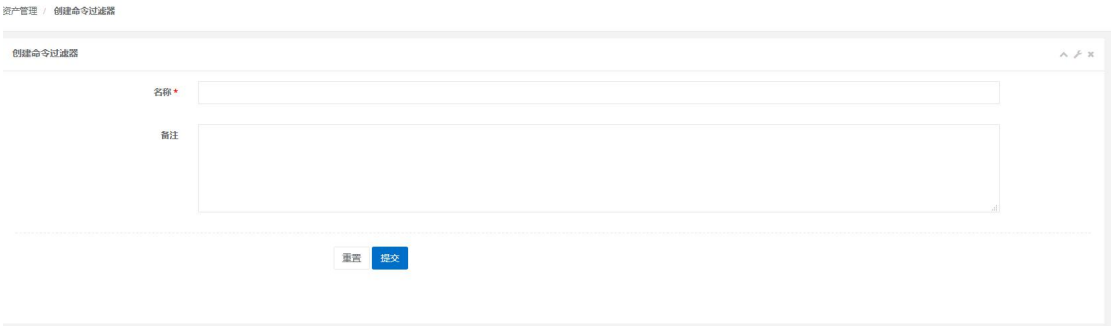
户登录资产，然后执行一个命令，这个命令需要被绑定过滤器的所有规则匹配，高优先级先被匹配。当一个规则匹配到了，如果规则的动作是允许,，这个命令会被放行；如果规则的动作是禁止，命令将会被禁止执行，否则就匹配下一个规则，如果最后没有匹配到规则，则允许执行。

5.6.1. 命令过滤列表



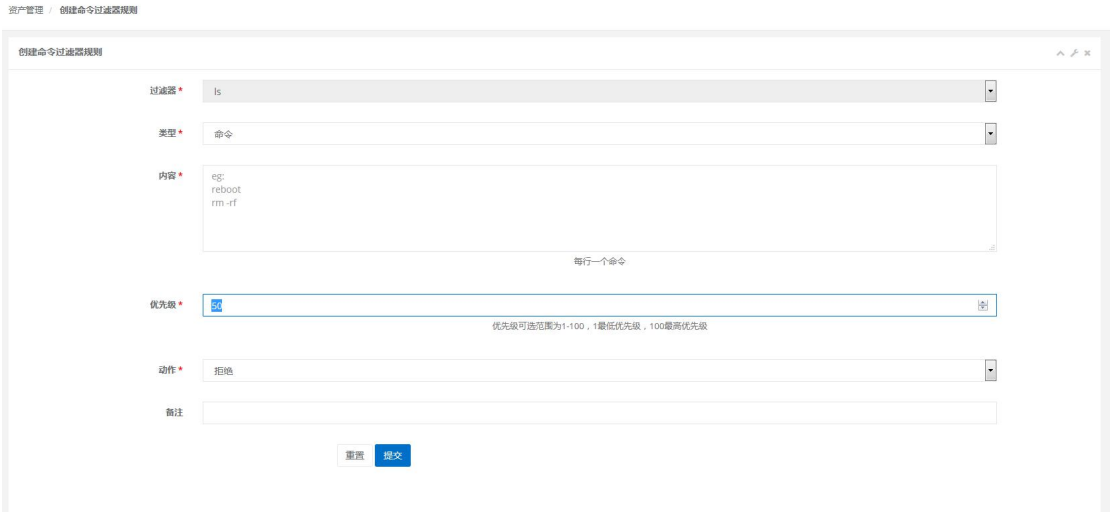
5.6.2. 创建命令过滤器

进入[命令过滤]，点击<创建命令过滤器>，跳转至创建页面，如图所示。

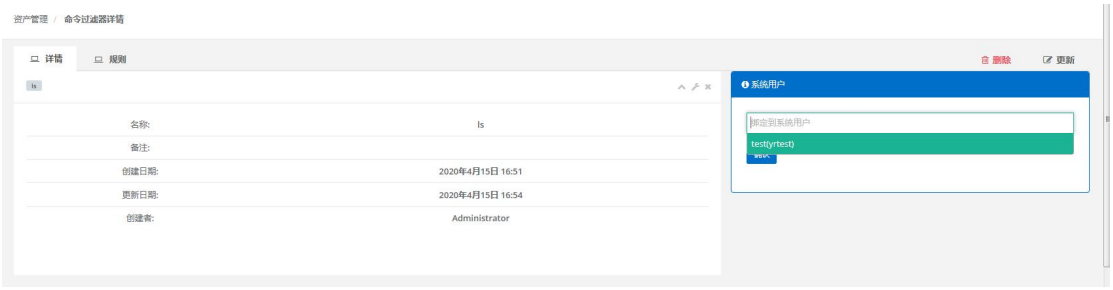


提交之后，列表中会出现刚刚创建的过滤器，点击过滤器名称，在过滤器详情页面点击<规则>

点击<创建规则>按钮，选择类型、内容和动作。执行动作包含：拒绝、允许，类型包括命令和正则表达式，内容框内每行输入一条命令。



在配置完规则之后，返回<详情>页，在页面右侧可以将此过滤器规则绑定到系统用户。

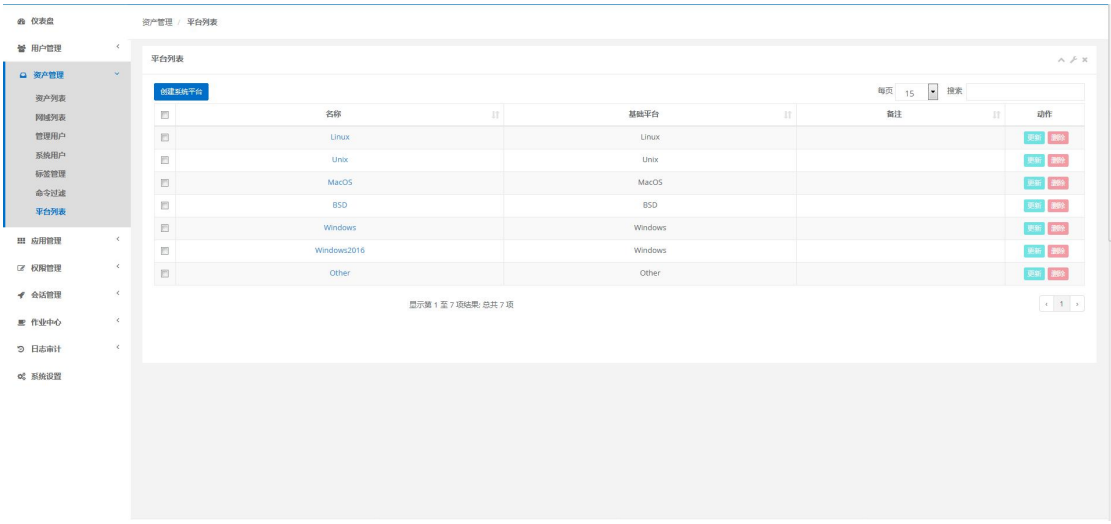


5.6.3. 规则查询

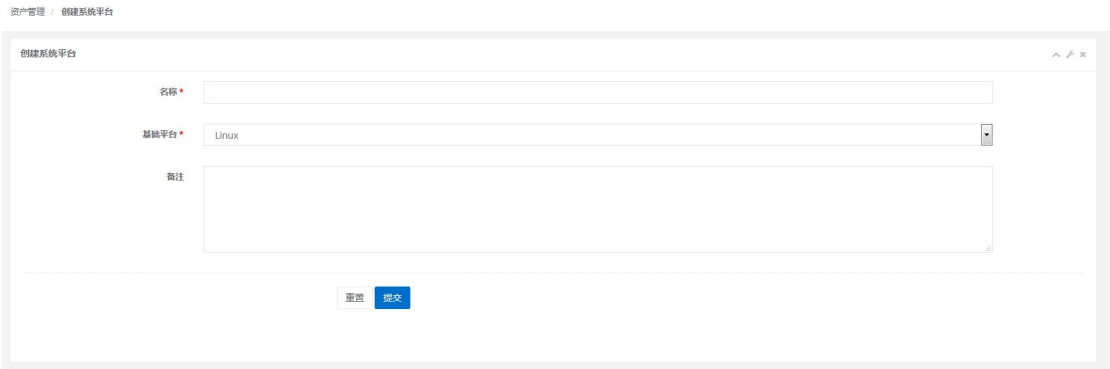
进入[命令过滤]，在右侧搜索输入框内容输入过滤器名称关键词，列表会自动显示符合条件的过滤器，如图。

5.7.平台列表

对于不同系统平台的自定义配置，用户可以自行创建不同参数的系统平台。在创建资产时可从平台列表中选择符合自己要求的系统平台，实现自定义功能。



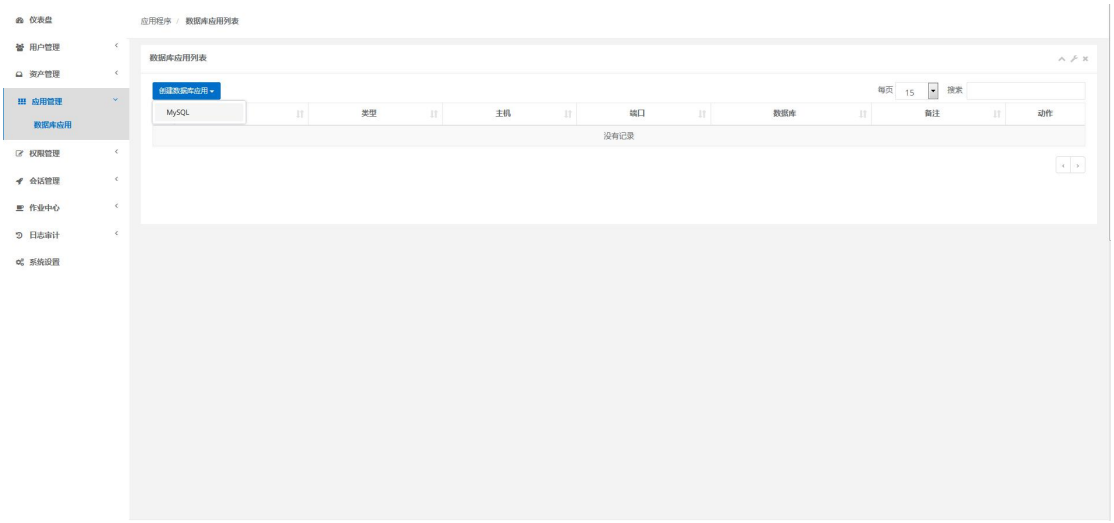
注意：系统内置的几个系统平台无法编辑也无法删除。用户只能根据已有的平台为基础自定义平台。



第六章. 应用管理

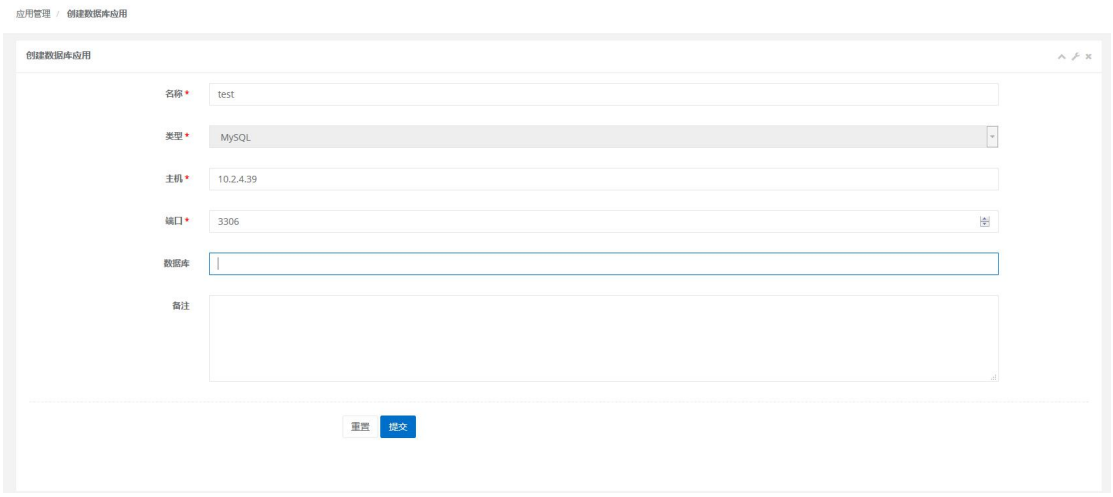
6.1. 数据库应用

为了方便用户对资产更细颗粒度的访问，云翼运维审计系统提供了数据库应用的管理。目前仅支持 MySQL 数据库。



6.2. 新建数据库应用

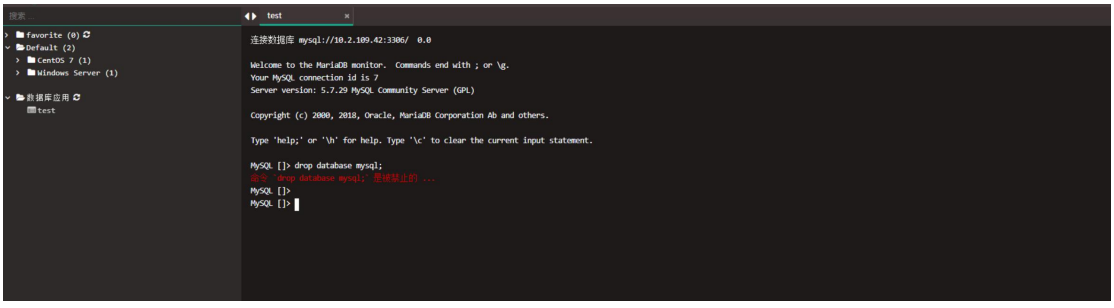
进入[应用管理/数据库应用]，点击<创建数据库应用>按钮，选择 MySQL，跳转至创建页面，如图。



填入正确的 MySQL 地址、端口和数据库名称后，点击<提交>。再进入[资产管理/系统用户]页面，创建一个用于连接该 MySQL 数据库的用户，这个用户需要与 MYSQL 数据库的用户保持一致，如下图。

最后进入[权限管理/数据库应用]页面，为用户分配数据库应用使用权限。点击<创建授权规则>按钮，跳转至创建规则页面，如下图。

最终的连接效果如下图。



第七章. 应用发布

7.1. 应用发布

7.2. 应用发布搭建方案

步骤 1 右击“这台电脑”，单击<属性>进入[系统]管理界面。

图 1 系统管理界面


系统
控制面板 ▸ 系统和安全 ▸ 系统
搜索控制面板
控制面板主页
设备管理器
远程设置
高级系统设置
查看有关计算机的基本信息
Windows 版本
Windows Server 2012 R2 Standard
© 2013 Microsoft Corporation。保留所有权利。
Windows Server 2012 R2
系统
处理器: Pentium(R) Dual-Core CPU E6500 @ 2.93GHz 2.93 GHz
安装内存(RAM): 3.00 GB
系统类型: 64 位操作系统，基于 x64 的处理器
笔和触摸: 没有可用于此显示器的笔或触控输入
计算机名、域和工作组设置
计算机名: windows2012
更改设置
计算机全名: windows2012.baoleijiyu.com
计算机描述:
域: baoleijiyu.com
另请参阅
操作中心
Windows 更新
Windows 激活
Windows 尚未激活。 阅读 Microsoft 软件许可条款
产品 ID: 00252-00055-00001-AA126
激活 Windows

步骤 2 单击<更改配置>进入[系统属性]界面。

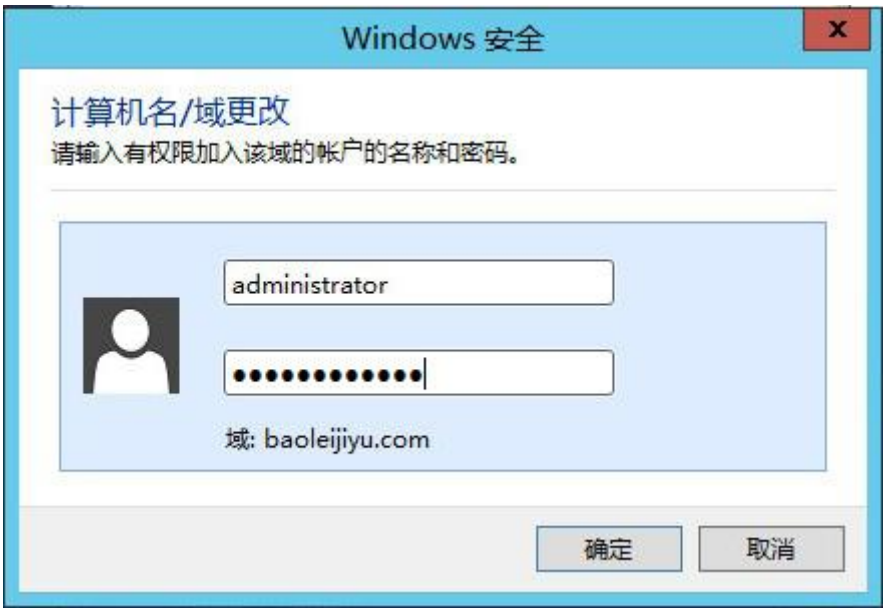
图 2 系统属性界面

步骤 3 单击<更改>进入[计算机名/域更改]界面，修改计算机名称、域名。

图 3 计算机名/域更改界面

步骤 4 单击<确定>后，提示输入域帐户和密码。

图 4 Windows 安



步骤 5 单击<确定>后，提示加入域成功。

图 5 域更改成功界面

步骤 6 单击<确定>后重启计算机即可。

7.2.1 安装远程桌面服务

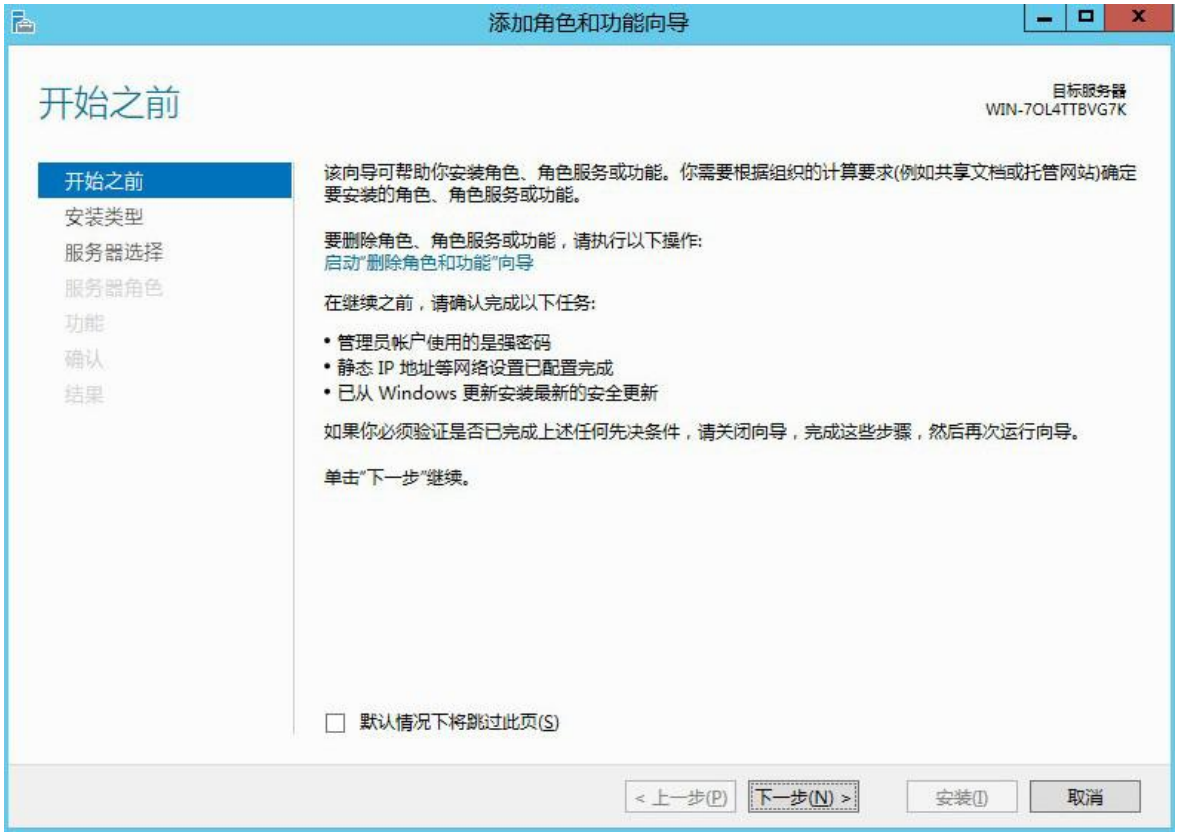
步骤 1 重启系统后，请使用 AD 域帐户和密码登录系统。

图 6 使用 AD 域帐户和密码登

步骤 2 进入[服务器管理器/仪表板]界面。

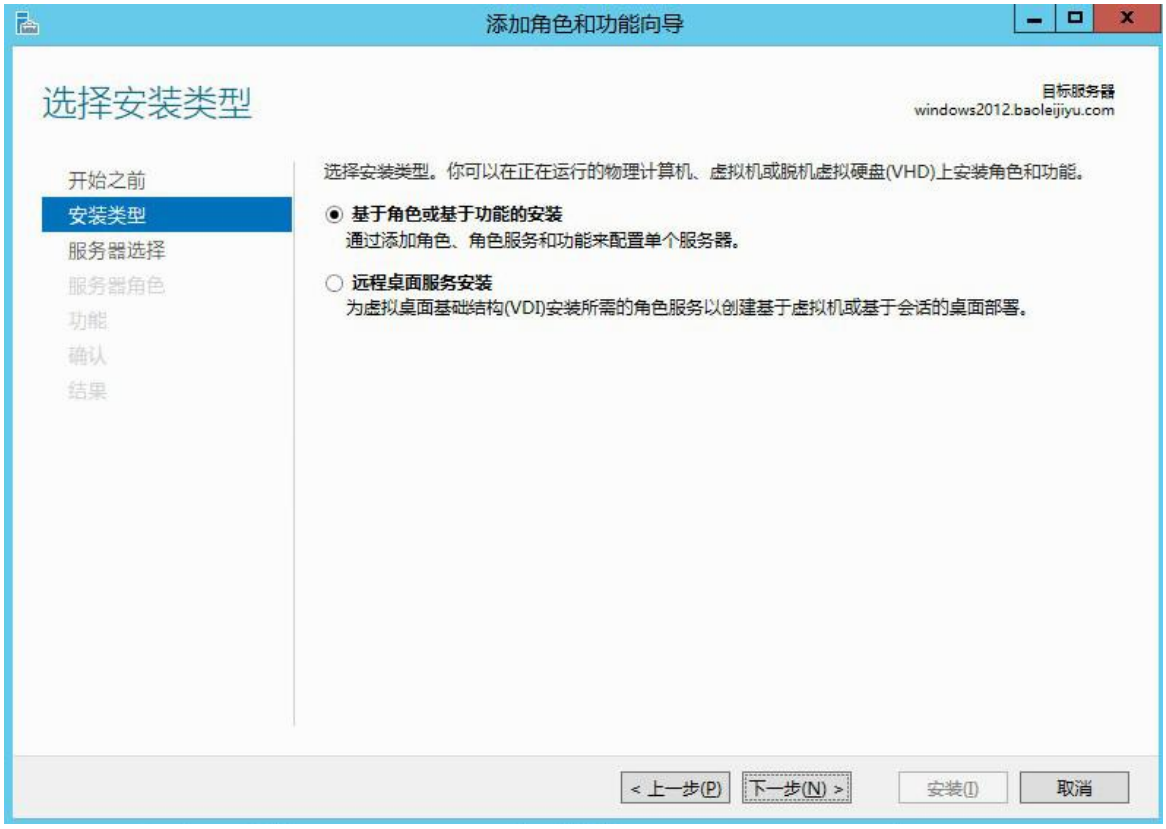
图 7 服务器管理器/仪表板界面

步骤 3 单击<添加角色和功能>进入“添加角色和功能向导”界面。

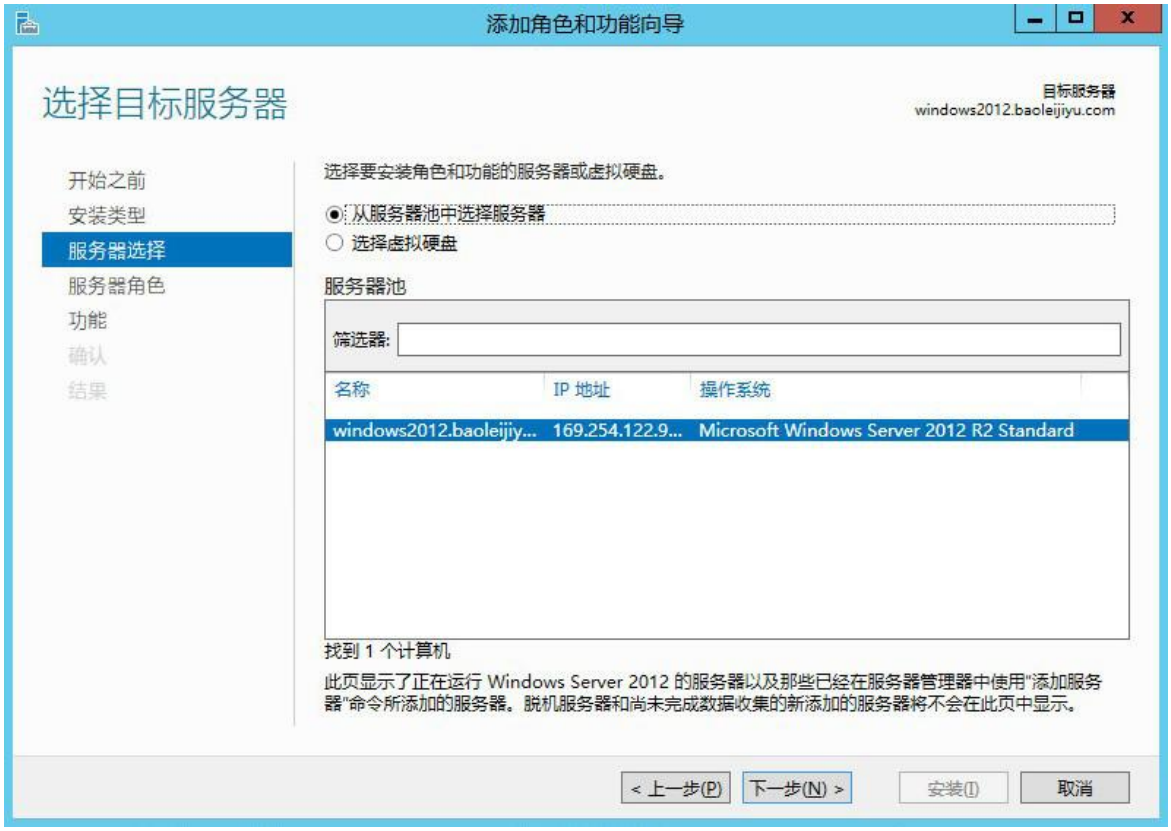


步骤 4 单击<下一步>进入安装类型界面，选择“基于角色或基于功能的安装”。

图 9 基于角色或基于功能的安

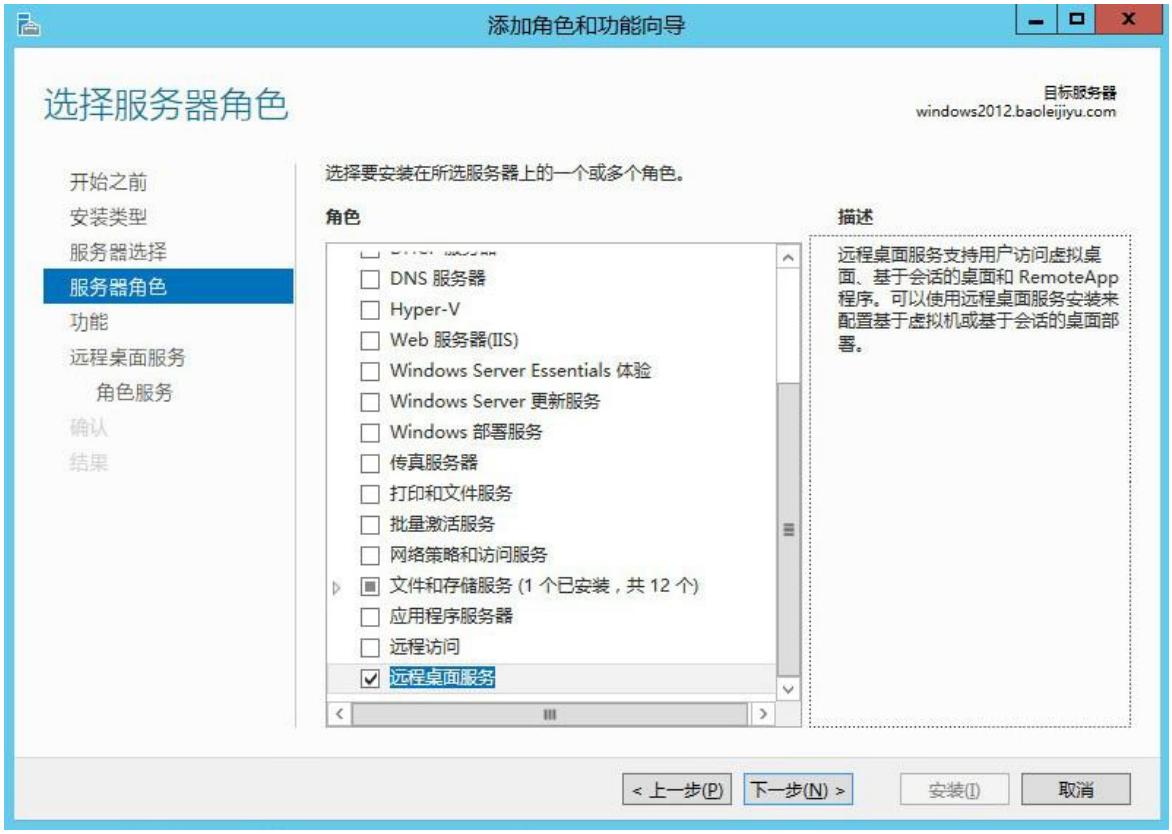


步骤 5 单击<下一步>进入服务器选择界面，选择“从服务器池中选择服务器”。

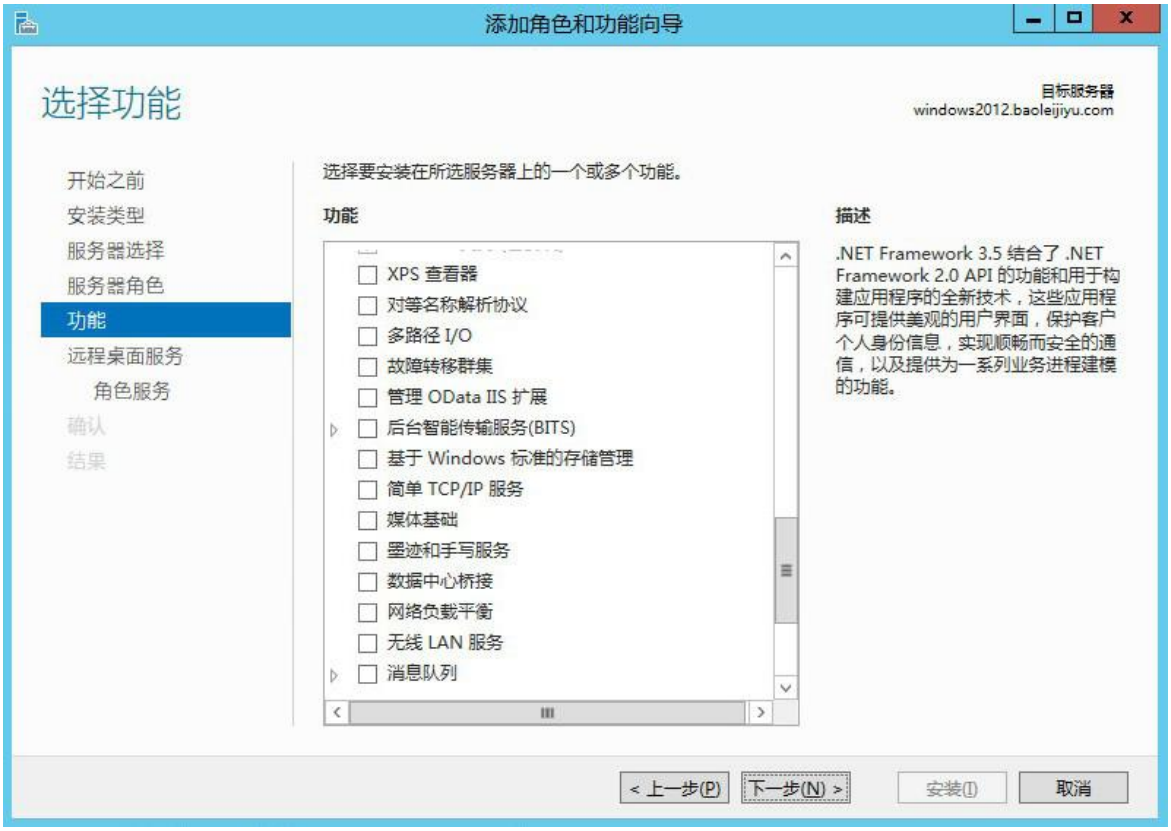


步骤 6 单击<下一步>进入服务器角色界面，勾选“远程桌面服务”。

图 11 选择远程桌面

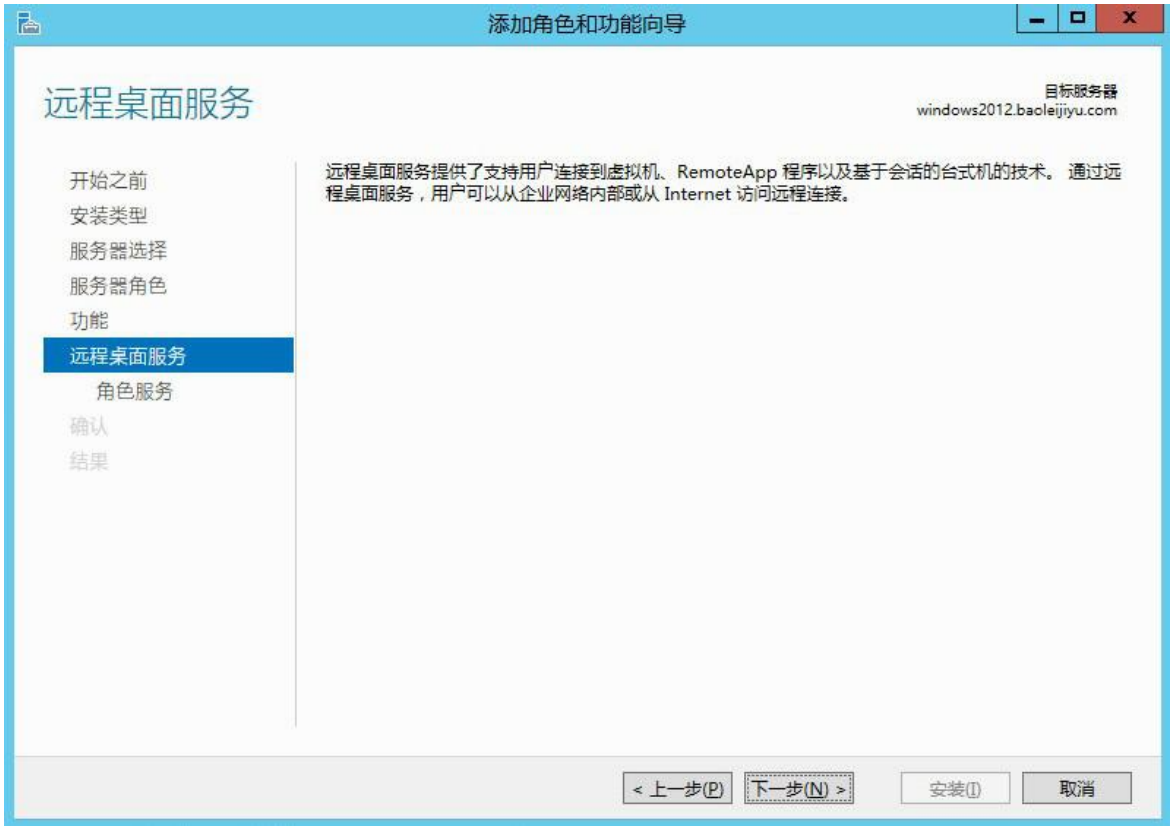


步骤 7 单击<下一步>进入功能界面，不选择任何功能项。

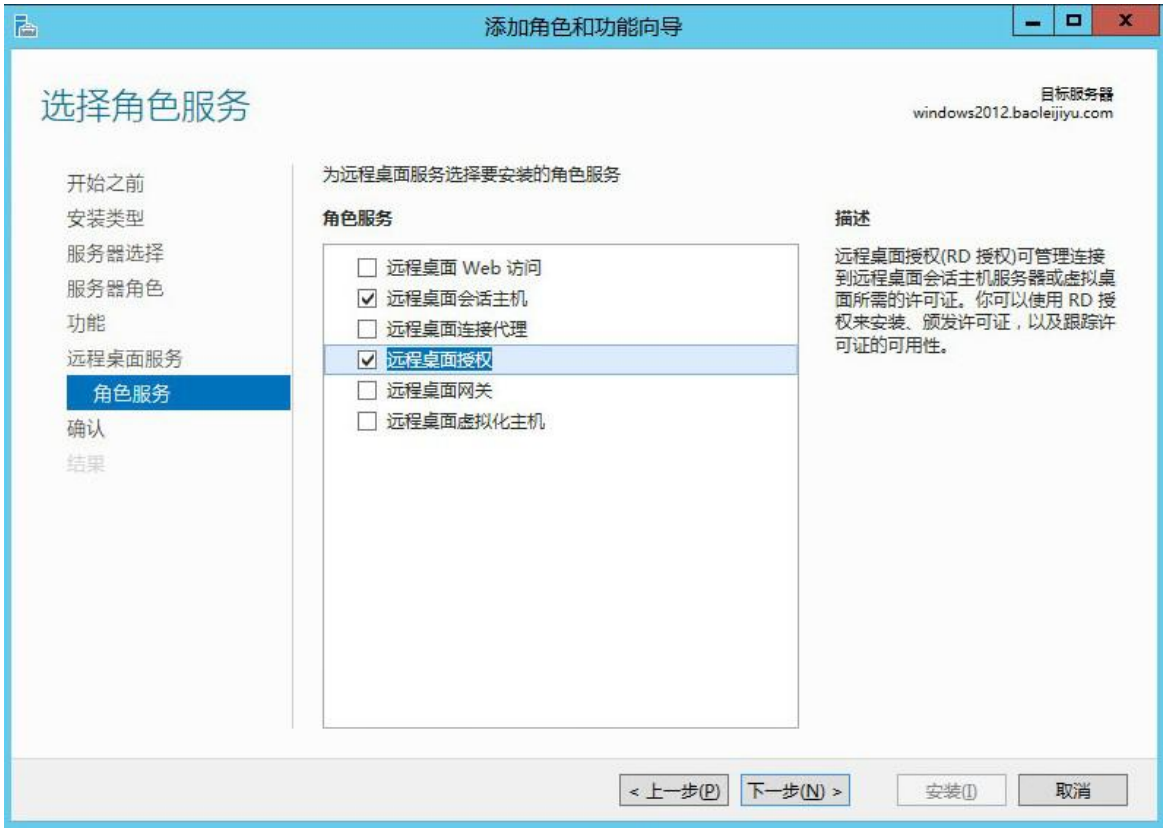


步骤 8 单击<下一步>进入远程桌面服务界面。

图 13 远程桌面服



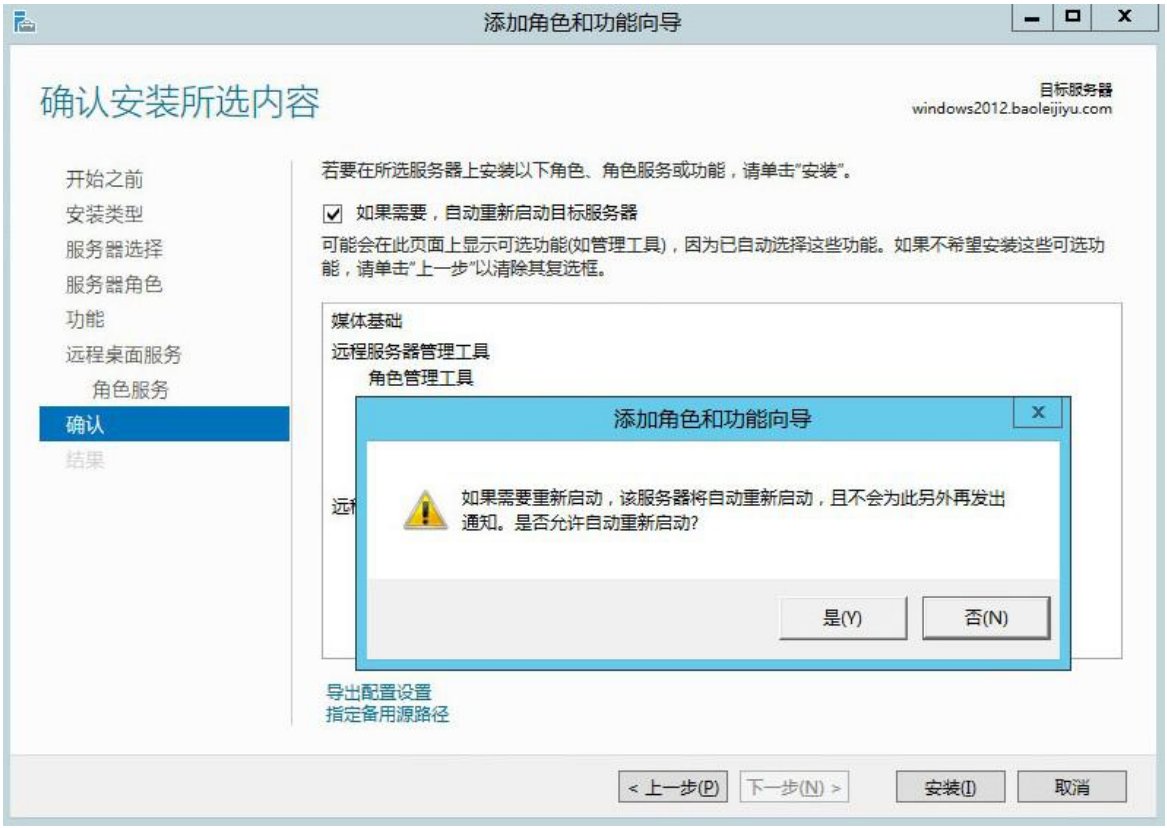
步骤 9 单击<下一步>进入角色服务界面，选择“远程桌面会话主机”和“远程桌面授权”。



步骤 10 单击<下一步>进入确认界面。

图 15 确

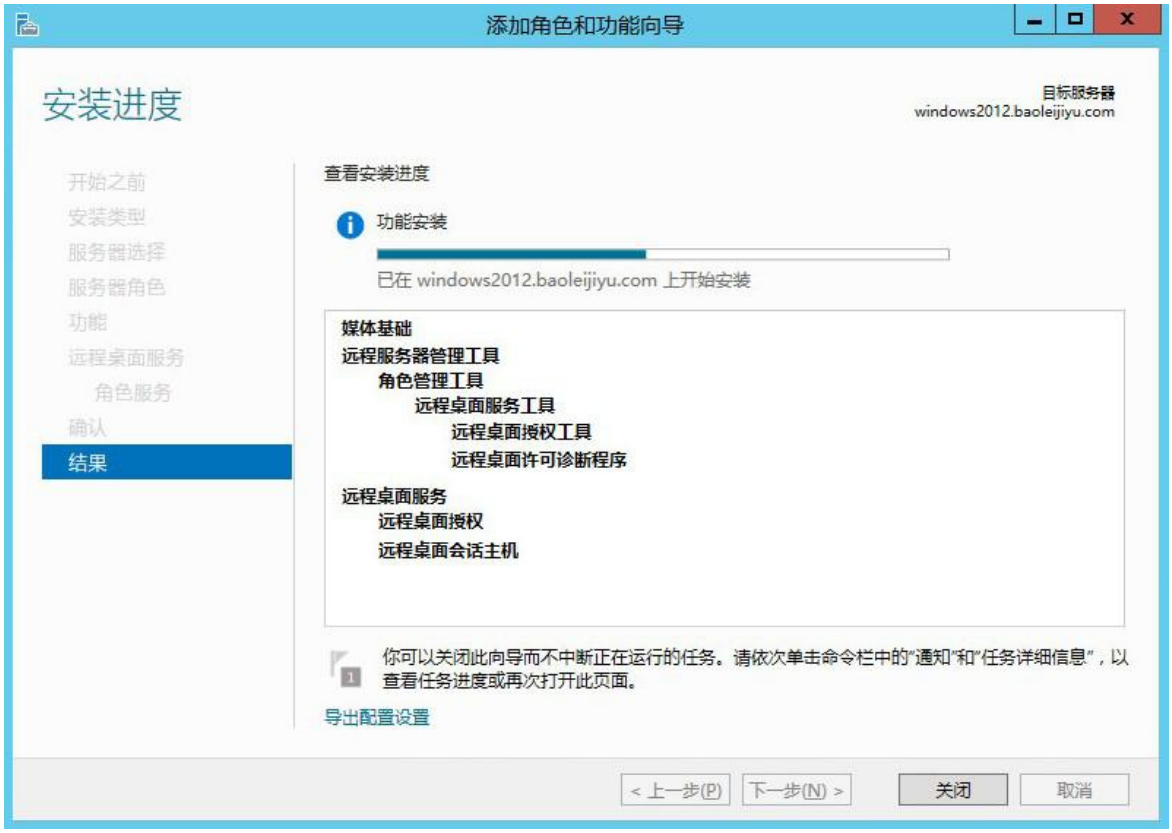
步骤 11 勾选“如果需要，自动重新启动目标服务器”，弹出提示窗口。


添加角色和功能向导
确认安装所选内容
目标服务器
windows2012.baoleijiyu.com
开始之前
安装类型
服务器选择
服务器角色
功能
远程桌面服务
角色服务
确认
结果
若要在所选服务器上安装以下角色、角色服务或功能，请单击"安装"。
如果需要，自动重新启动目标服务器
可能会在此页面上显示可选功能(如管理工具)，因为已自动选择这些功能。如果不希望安装这些可选功能，请单击"上一步"以清除其复选框。
媒体基础
远程服务器管理工具
角色管理工具
添加角色和功能向导
如果需要重新启动，该服务器将自动重新启动，且不会为此另外再发出通知。是否允许自动重新启动?
是(Y)
否(N)
导出配置设置
指定备用源路径
< 上一步(P)
下一步(N) >
安装(I)
取消

步骤 12 单击<是>即可。

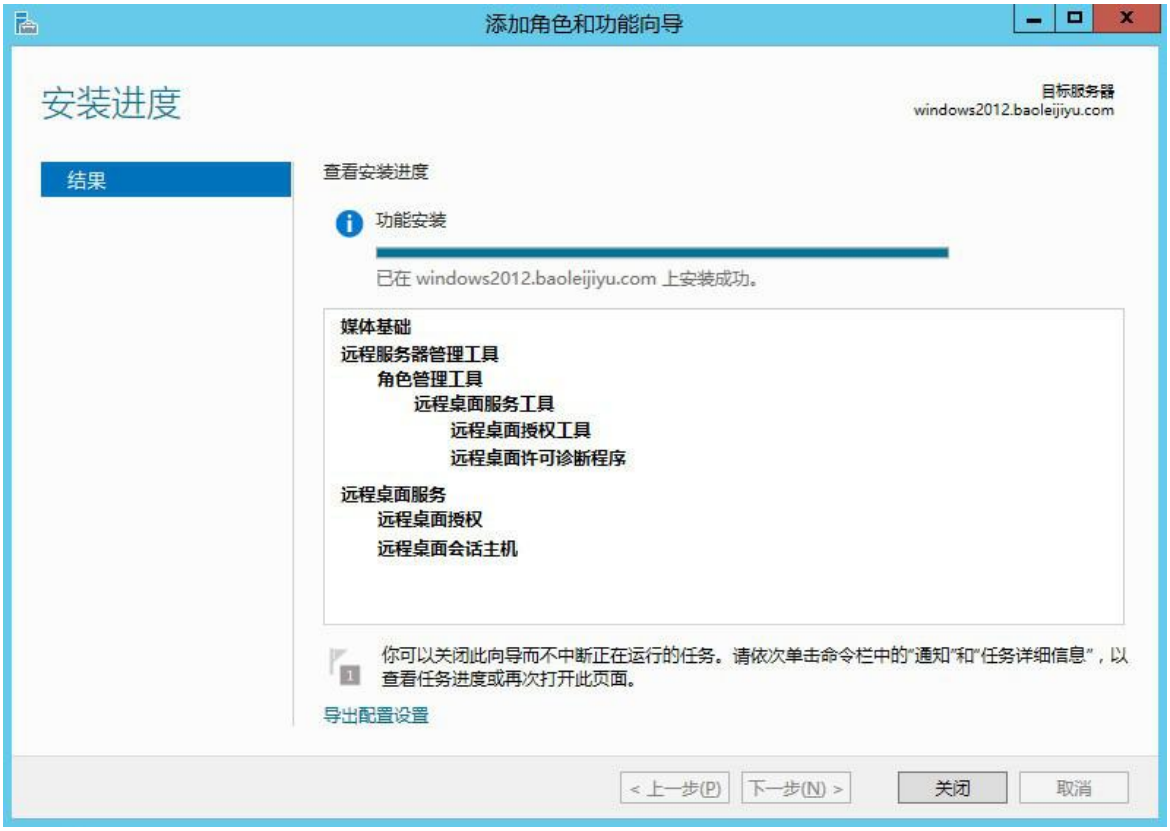
图 17 确

步骤 13 单击<安装>进入安装进度界面。



步骤 14 等待安装完成后，系统自动重新启动，并重新使用 AD 域帐户和密码登录系统。**步骤 15** 进入系统后，自动自动弹出安装进度，安装完成后，单击<关闭>即可。

图 19 安



7.2.2 安装 RemoteApp 服务

步骤 1 进入[服务器管理器/远程桌面服务/概述]界面中，可以看到说明需要安装“远程桌面服务”。

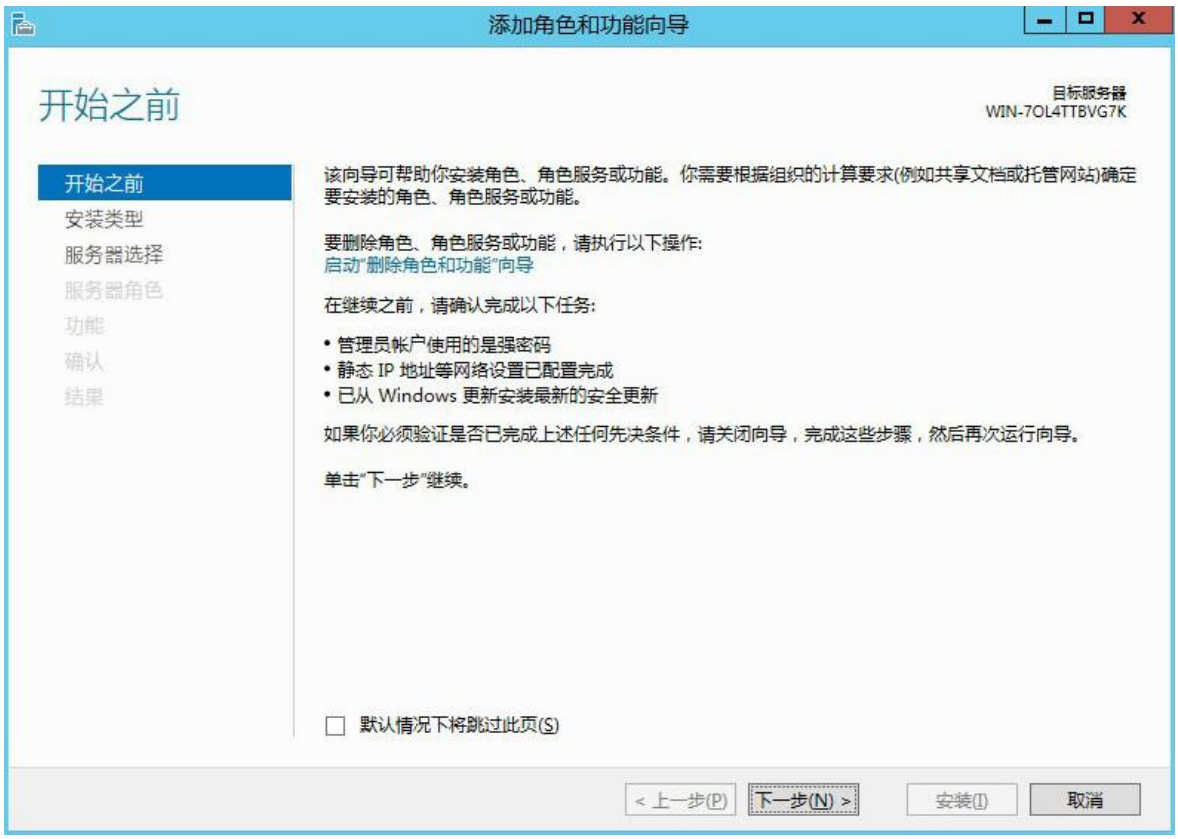
图 20 服务器管理器界面

步骤 2 进入[服务器管理器/仪表板]界面。

图 21 服务器管理器/仪表

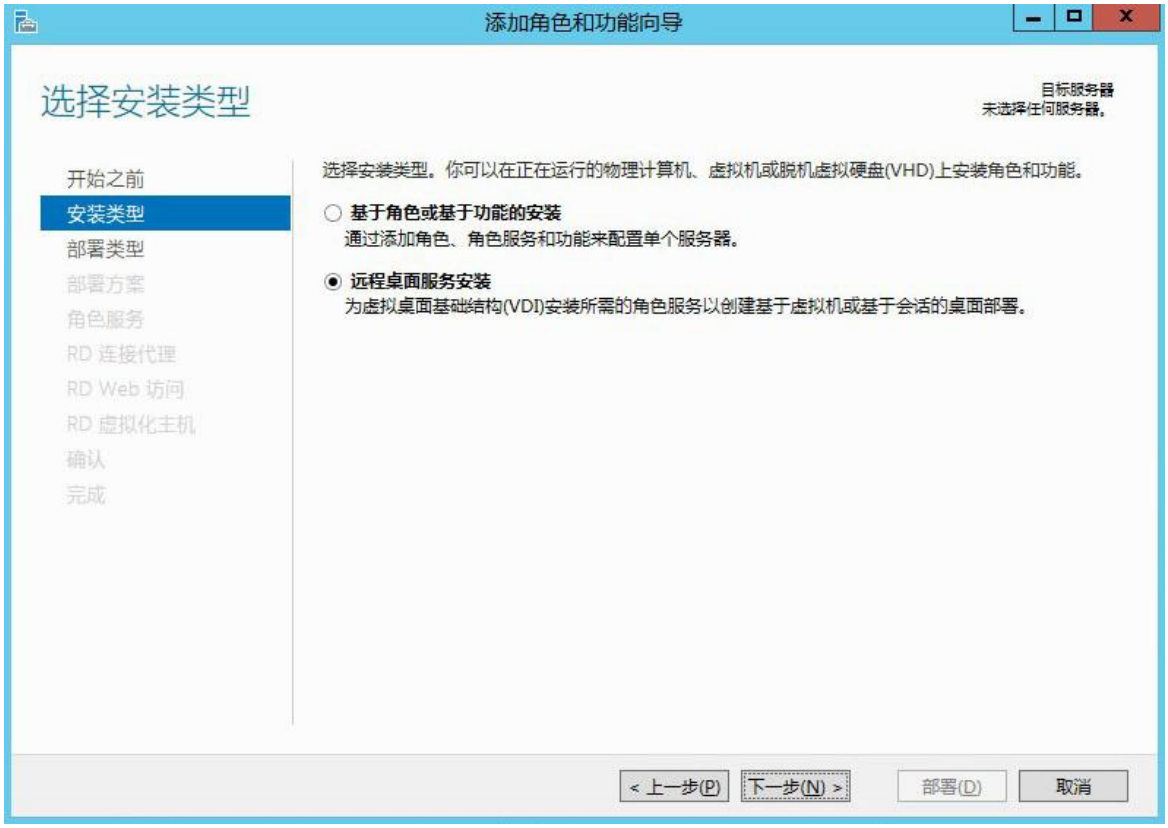
步骤 3 单击<添加角色和功能>进入添加角色和功能向导界面。

图 22 添加角色和功能向导界面

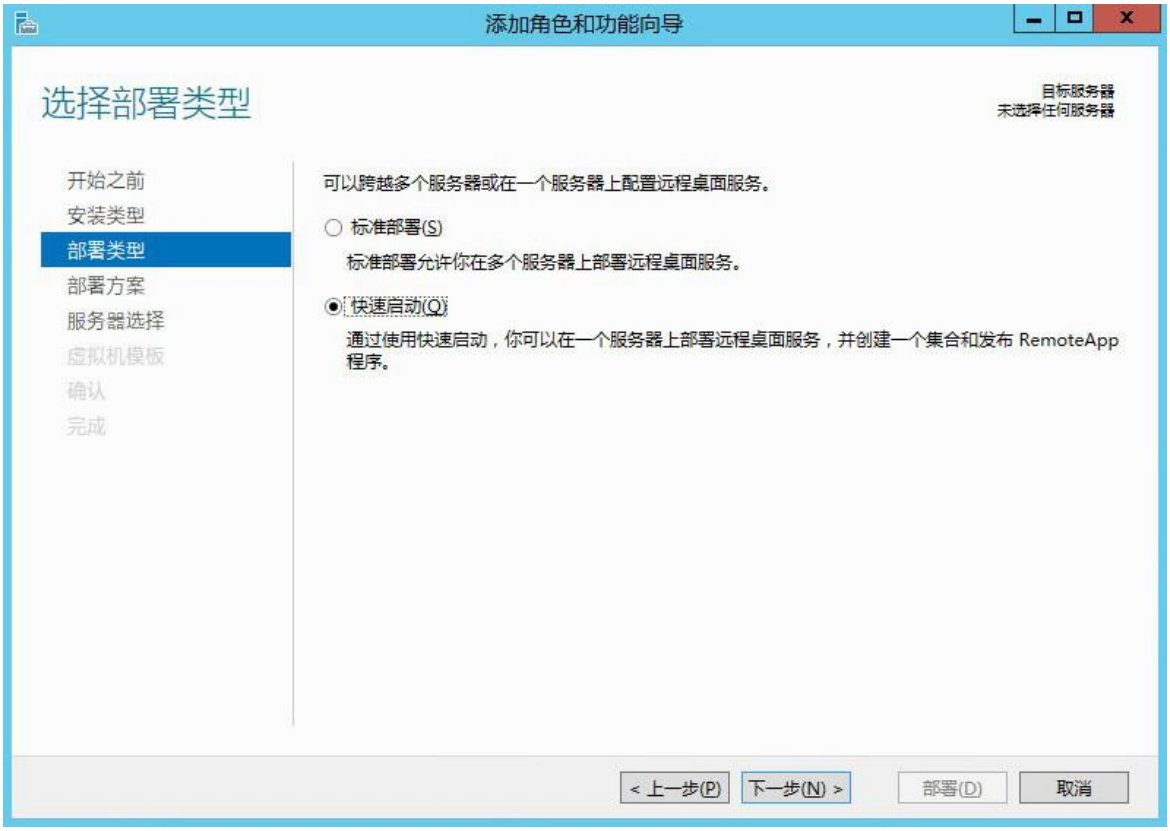


步骤 4 单击<下一步>进入安装类型界面，选择“远程桌面服务安装”。

图 23 远程桌面服务安

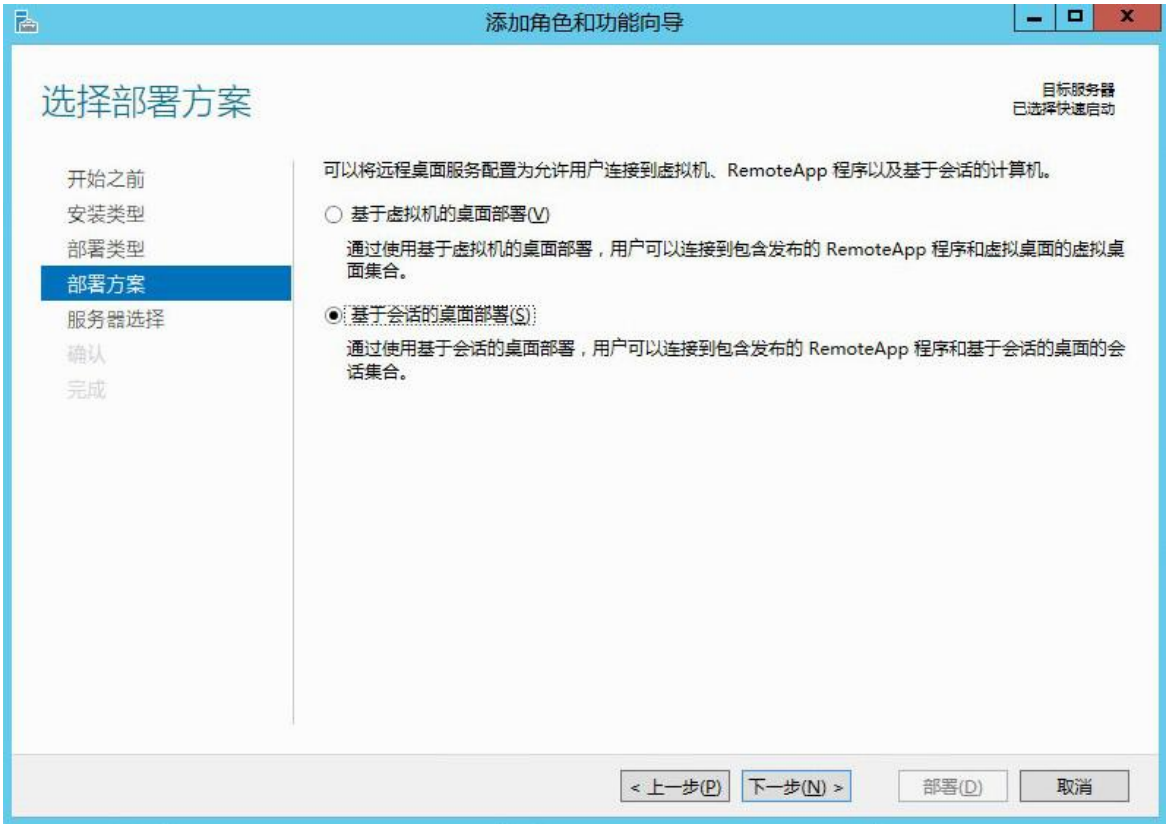


步骤 5 单击<下一步>进入部署类型界面，选择“快速启动”。

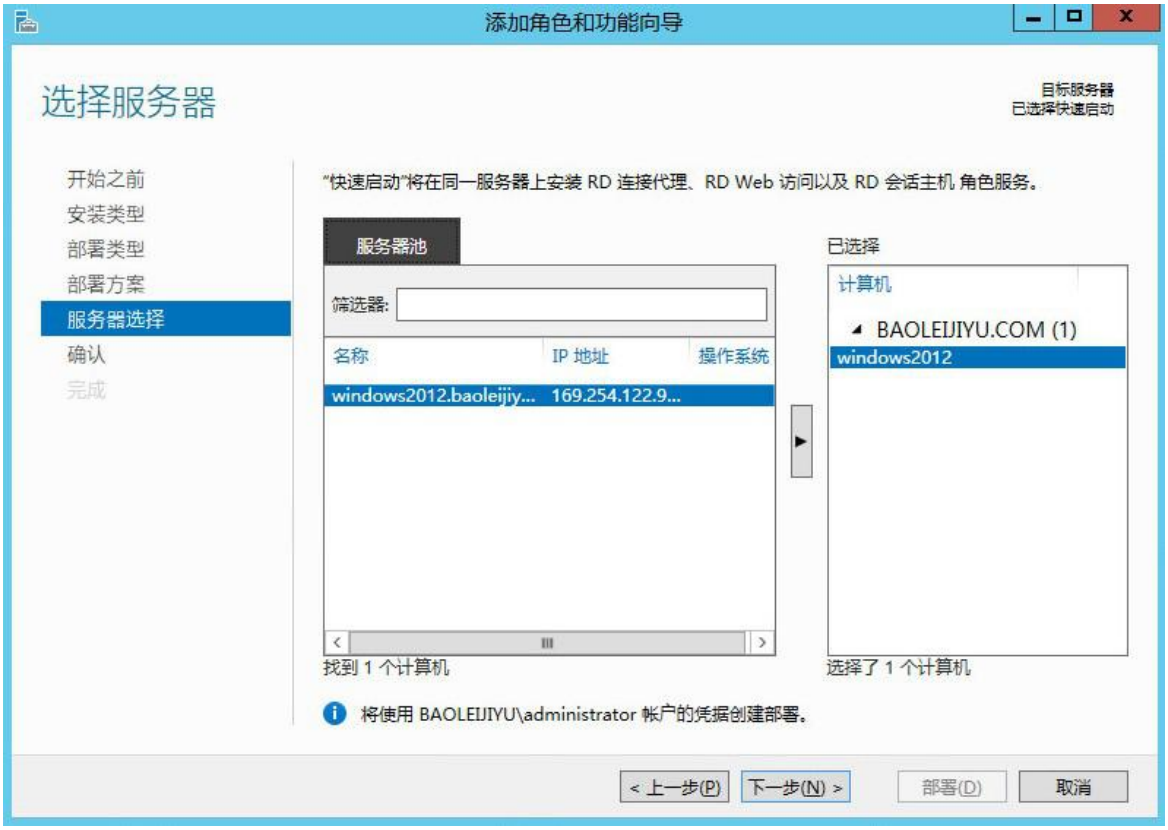


步骤 6 单击<下一步>进入部署方案，选择“基于会话的桌面部署”。

图 25 基于会话的桌面部

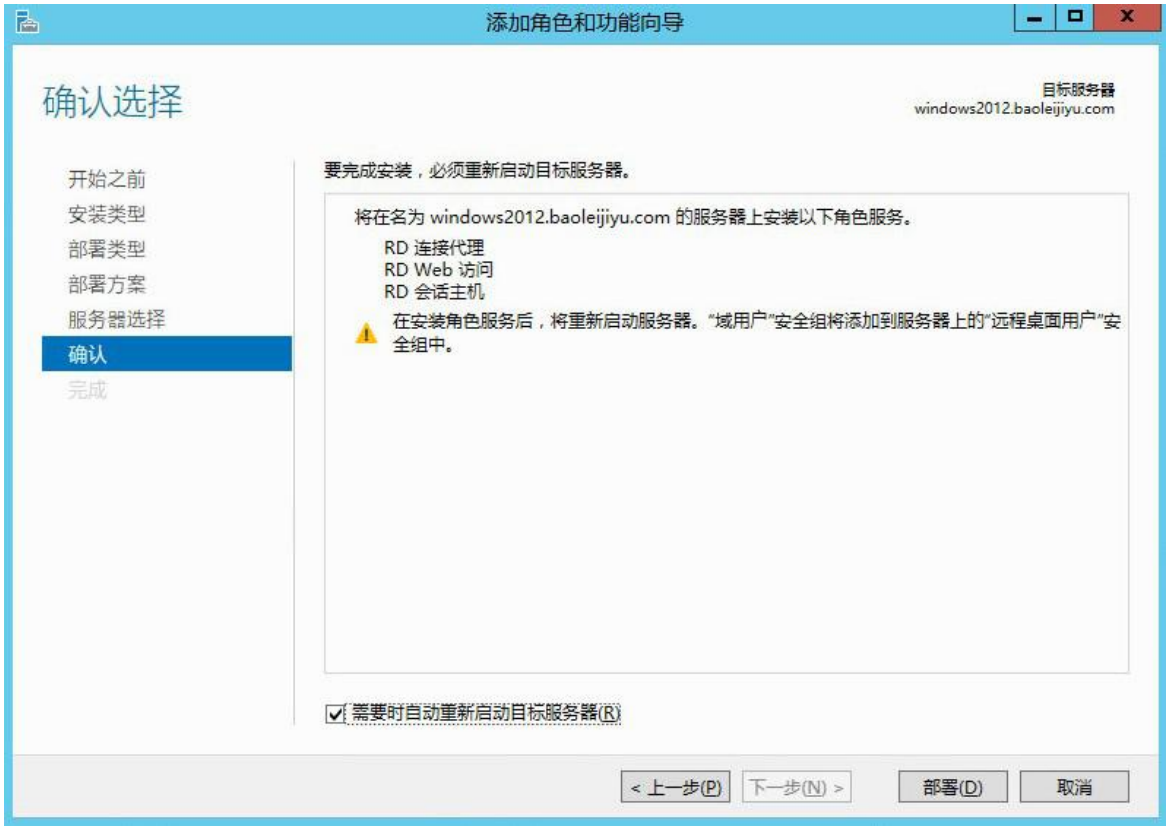


步骤 7 单击<下一步>进入服务器选择界面，将本地服务器移至右侧。

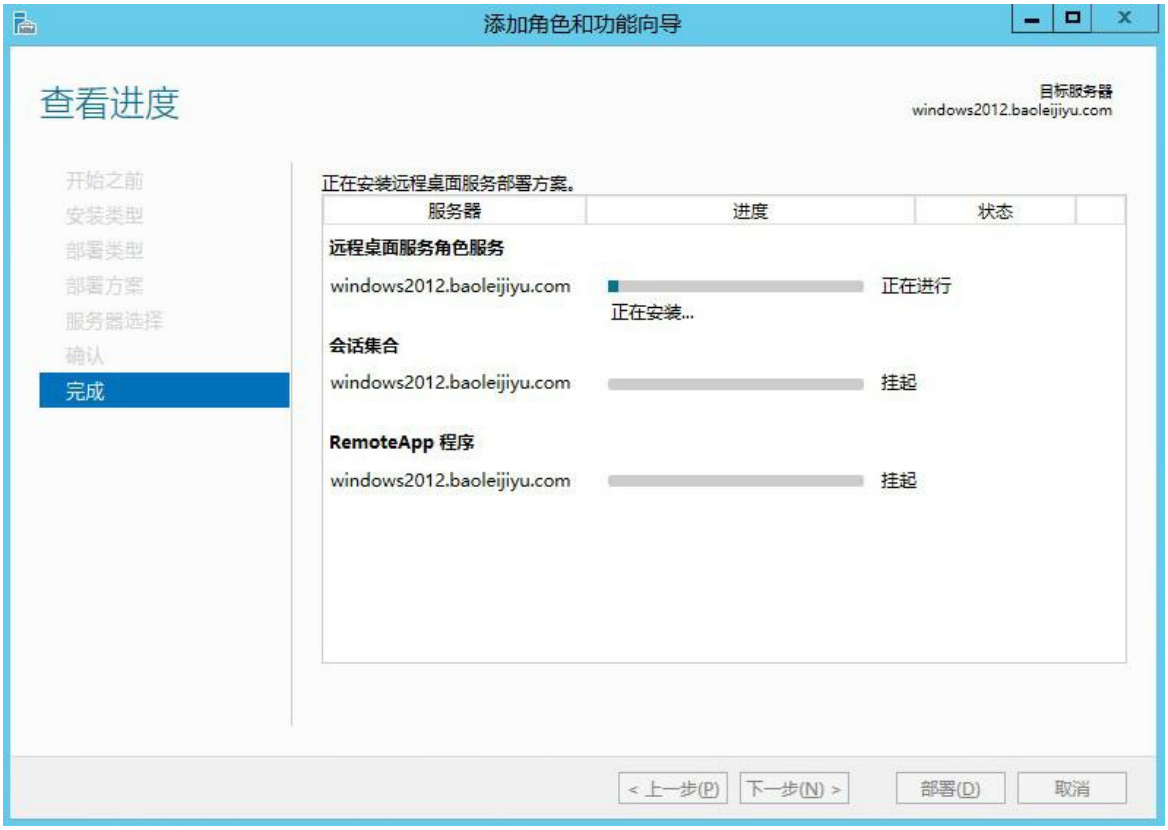


步骤 8 单击<下一步>进入确认界面。

图 27 确

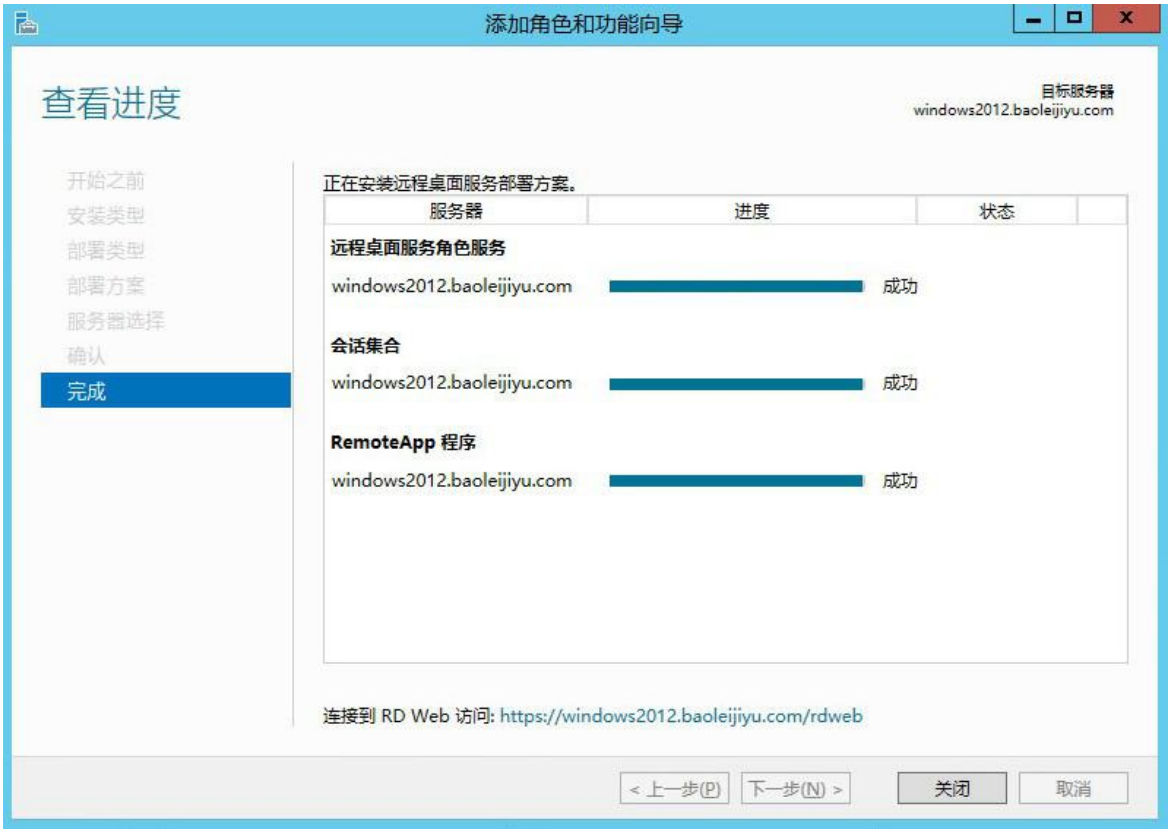


步骤 9 单击<部署>进入安装进度界面。



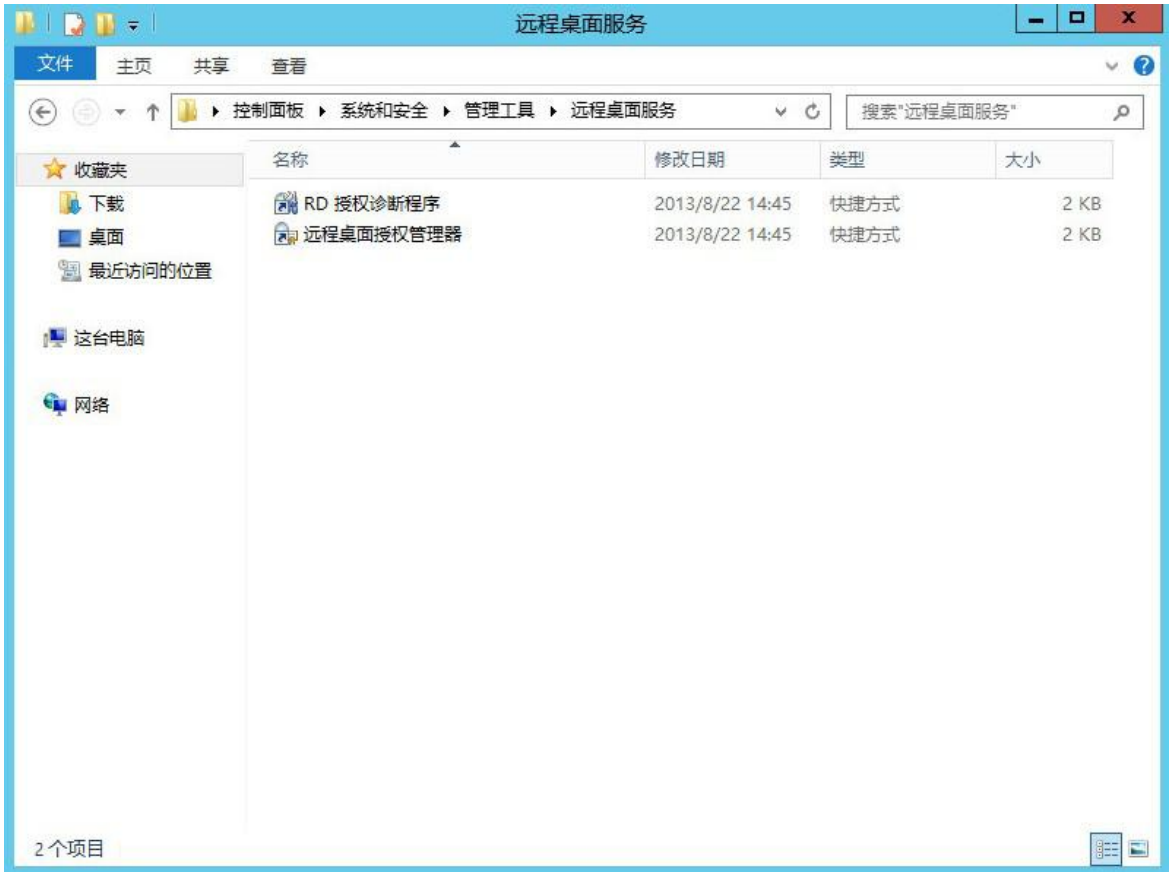
步骤 10 等待自动安装完成后，单击<关闭>即可。

图 29 关



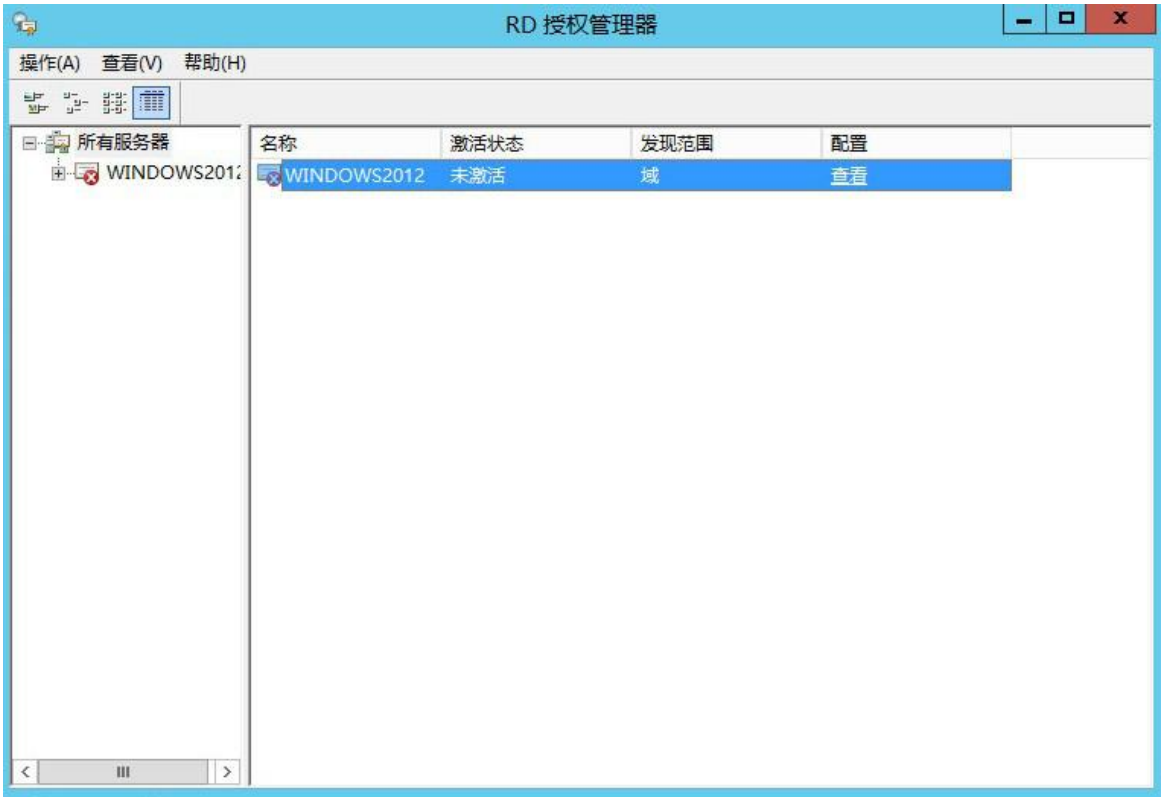
7.2.3 远程授权桌面

步骤 1 进入[控制面板/系统和安全/管理工具/远程桌面服务]界面。



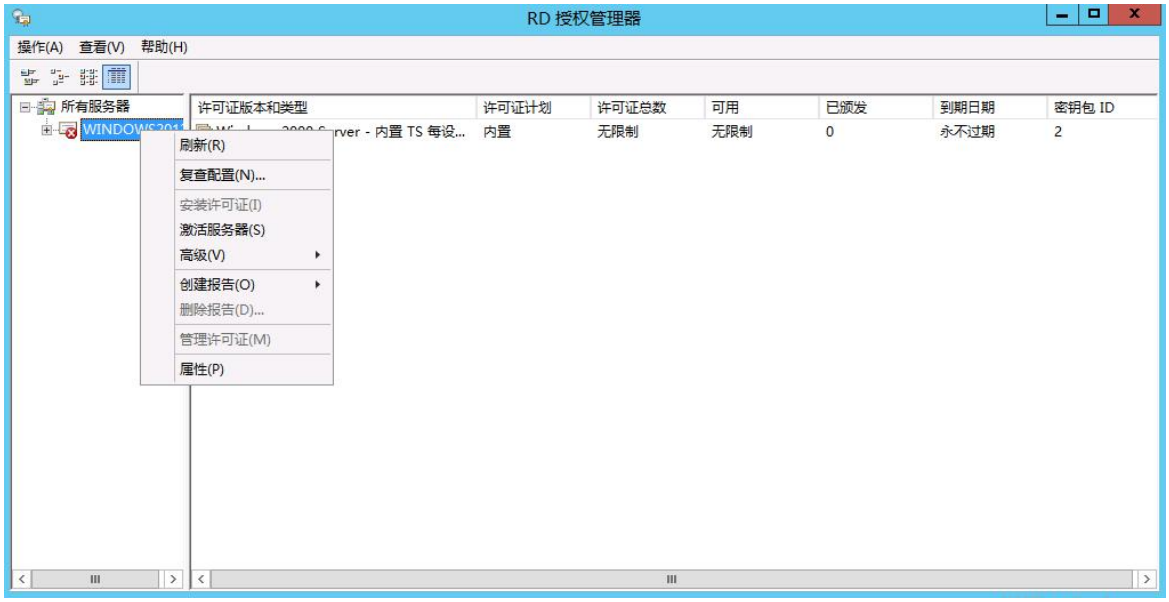
步骤 2 双击<远程桌面授权管理器>进入 RD 授权管理器界面。

图 31 RD 授权管理



步骤 3 右击计算机名称，显示可选项。

图 32 可选项界面



步骤 4 单击<激活服务器>进入服务器激活向导界面。

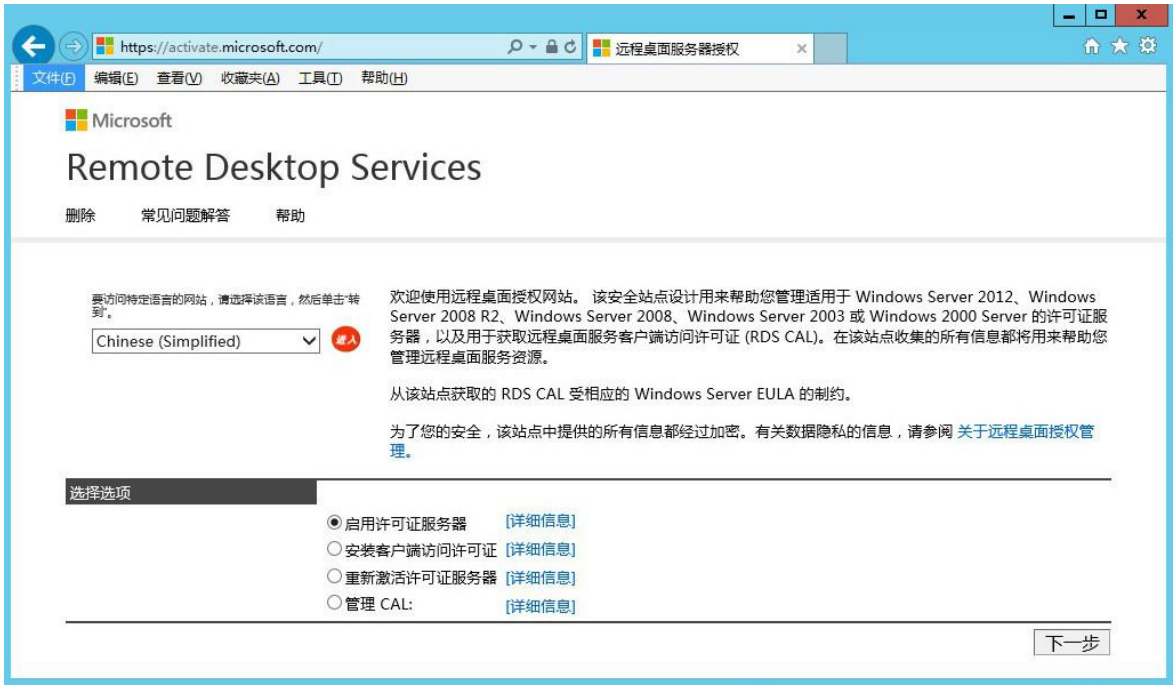
图 33 服务器激活向

步骤 5 单击<下一步>进入连接方法选择界面。

步骤 6 单击<下一步>进入许可证服务器激活界面。

图 35 许可证服务器激

步骤 7 使用一台可以上网的电脑，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”。



步骤 8 单击<下一步>进入 RDS 授权信息填写页面，输入 windwos server 2012 的正确产品 ID 号、公司名称、国家(地区)。

图 36 RDS 授

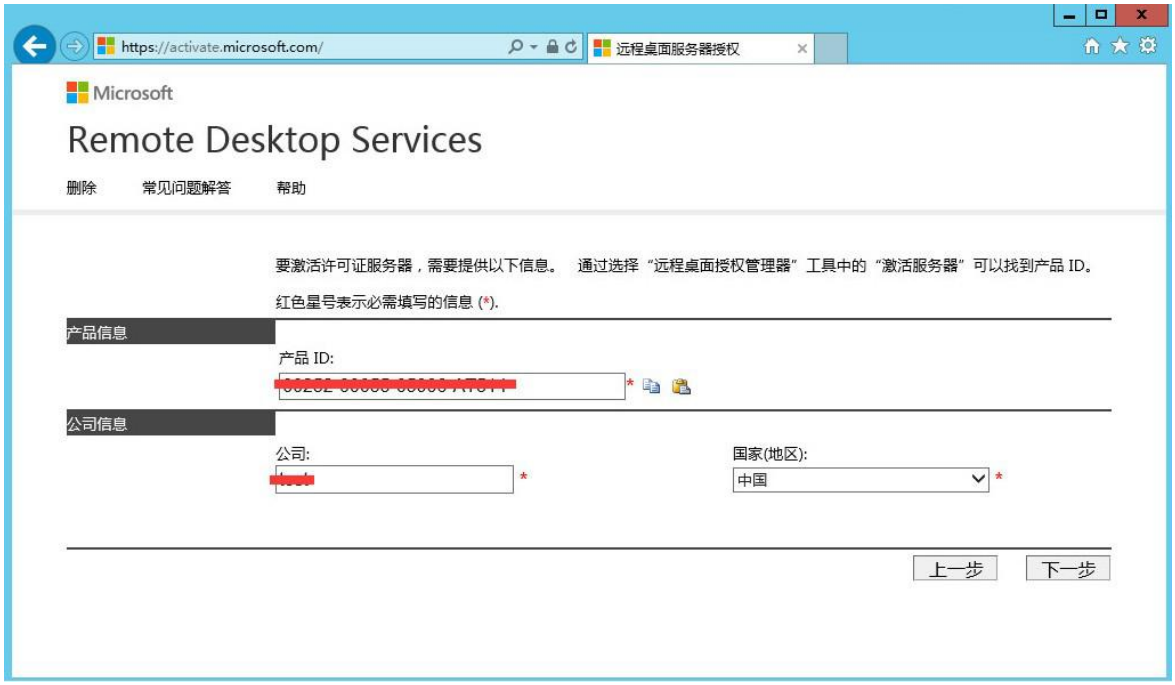
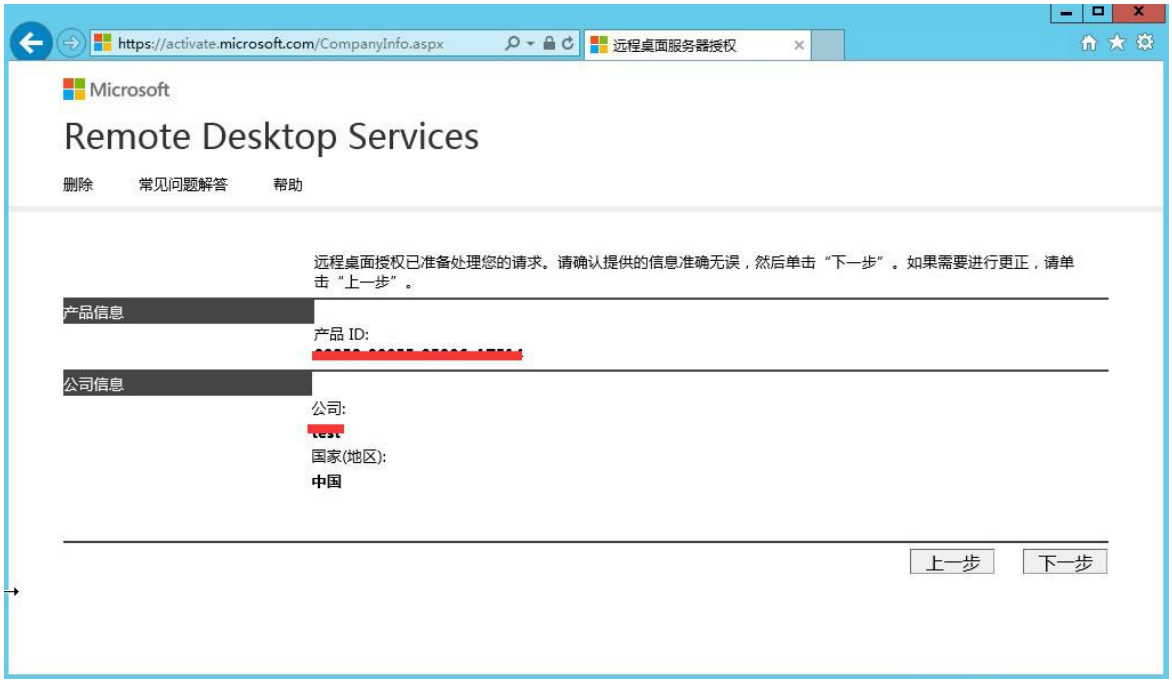


图 37 RDS 授权信息填写页面

步骤 9 单击<下一步>进入信息确认

页面。



步骤 10 单击<下一步>RDS 授权一个许可证服务器 ID 号，将此 ID 号复制并保存好。

图 38 信息确

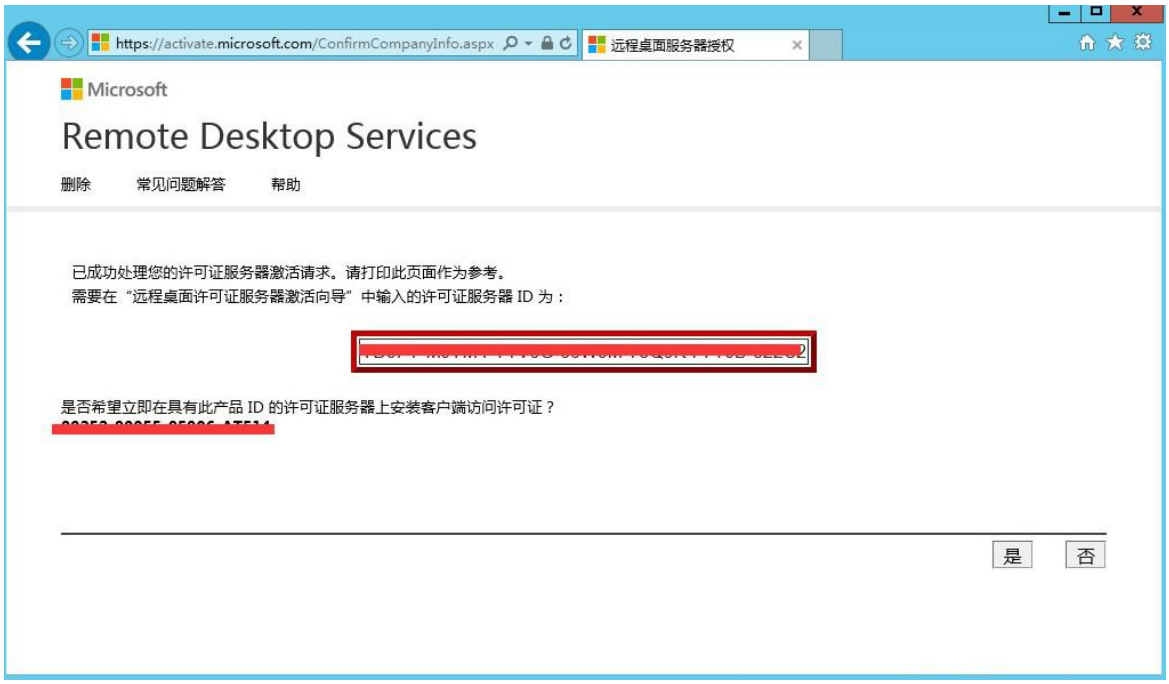
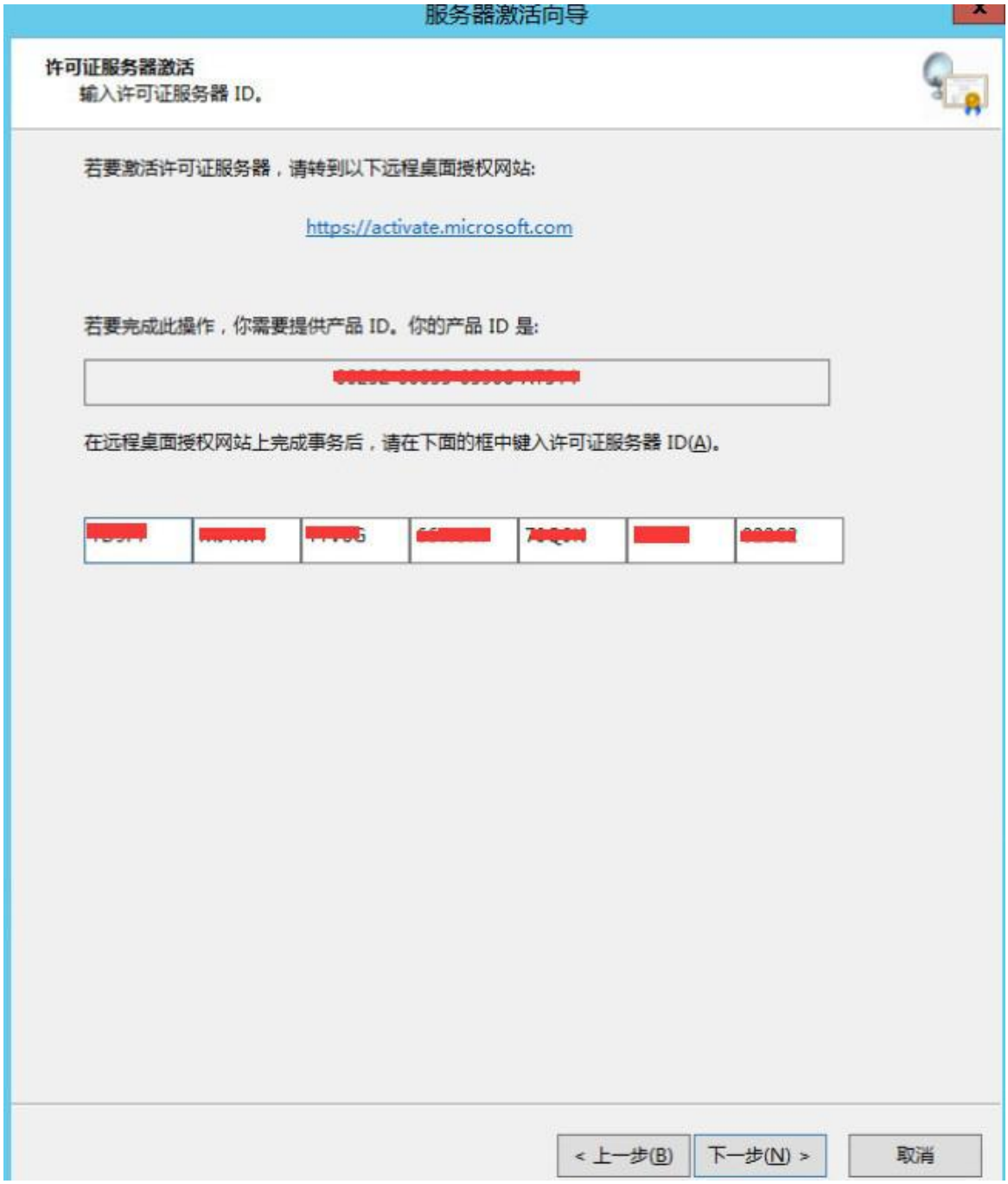


图 39 许可证服务器 ID 号界面

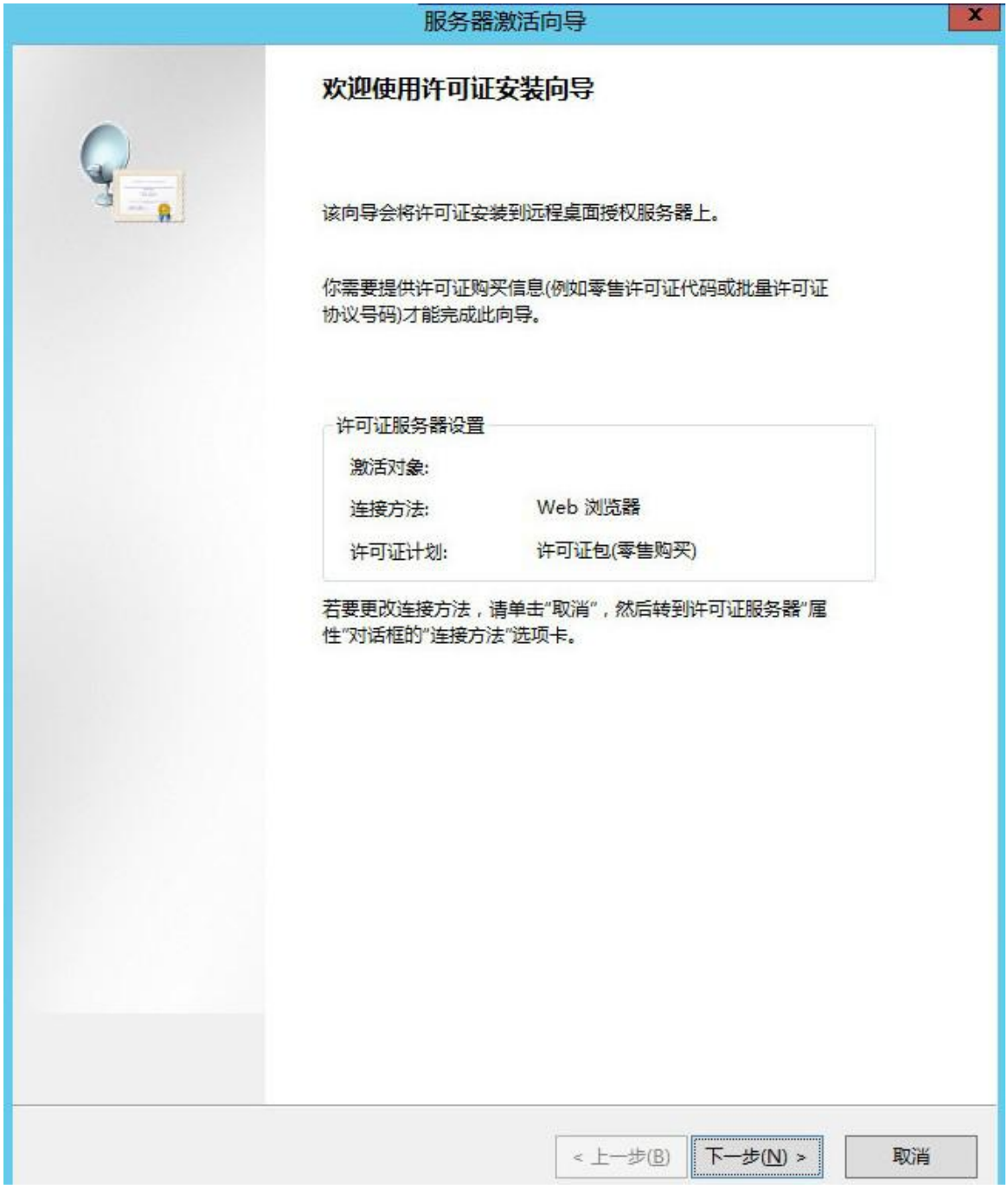
步骤 11 返回许可证服务器激活界面，将许可证服务器 ID 号填写进去。



步骤 12 单击<下一步>进入正在完成服务器激活向导。

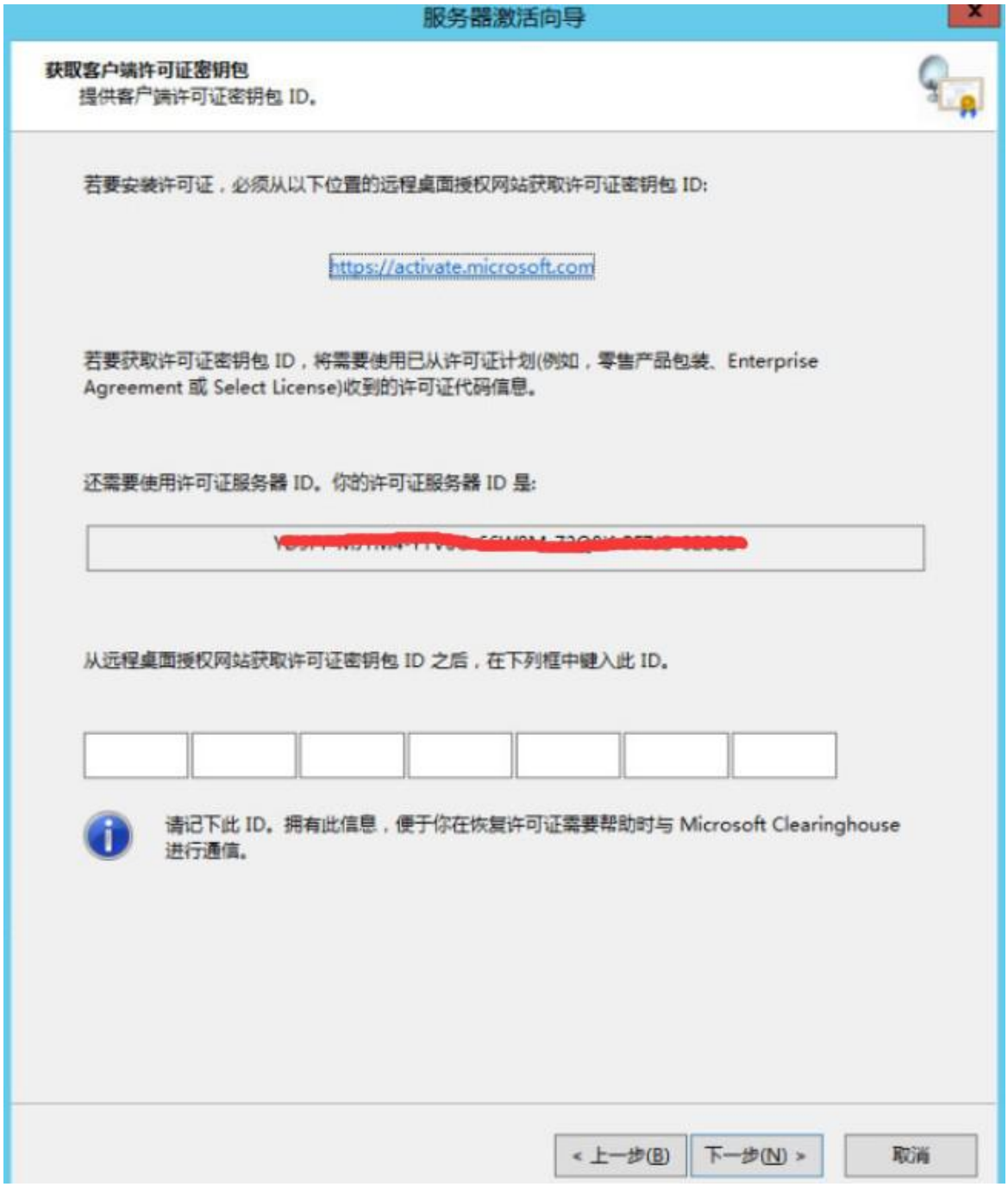
图 41 完成服务器激

步骤 13 单击<下一步>进入许可证安装向导界面。

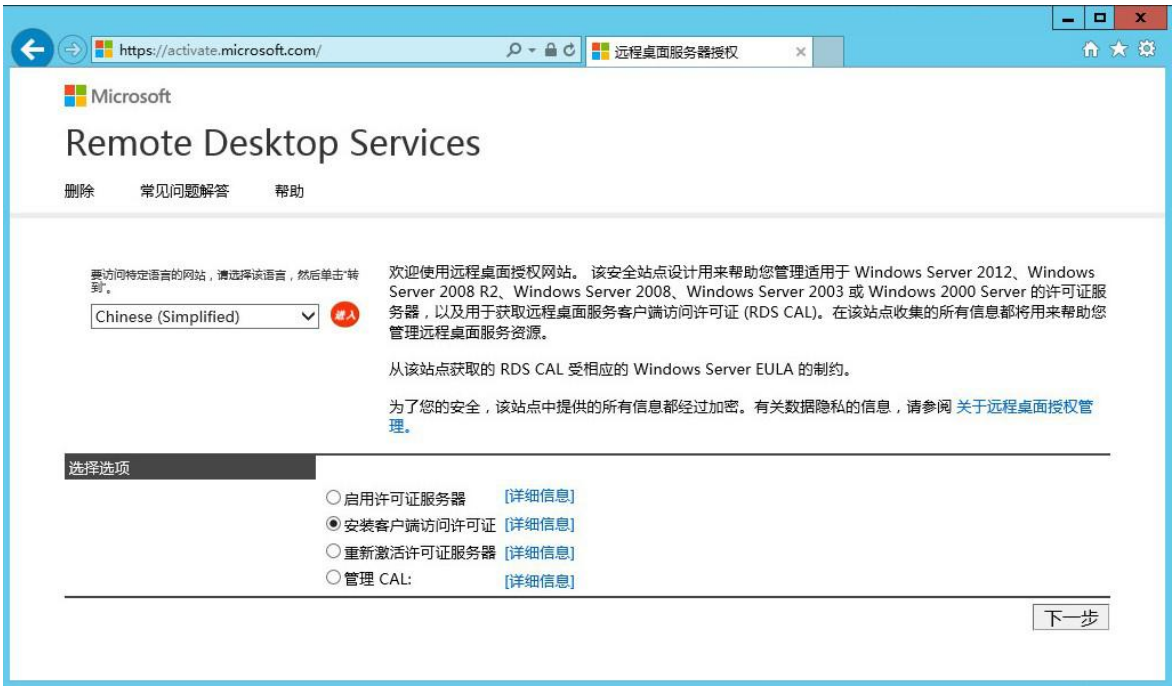


步骤 14 单击<下一步>进入获取客户端许可证密钥包界面。

图 43 获取客户端许可证密钥



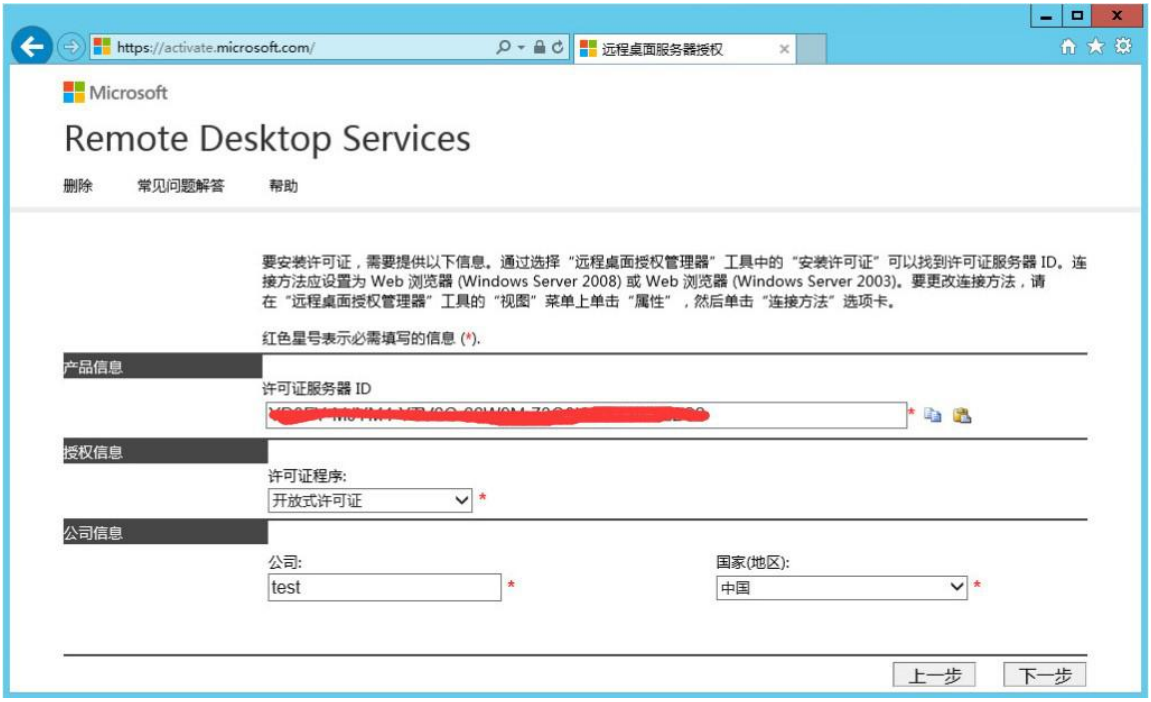
步骤 15 使用一台可以上网的电脑，在浏览器中输入 https://activate.microsoft.com 进入 RDS 授权页面， 选择“安装客户端许可证”。



步骤 16 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 号、选择许可证程序、公司名称、国家(地区)。

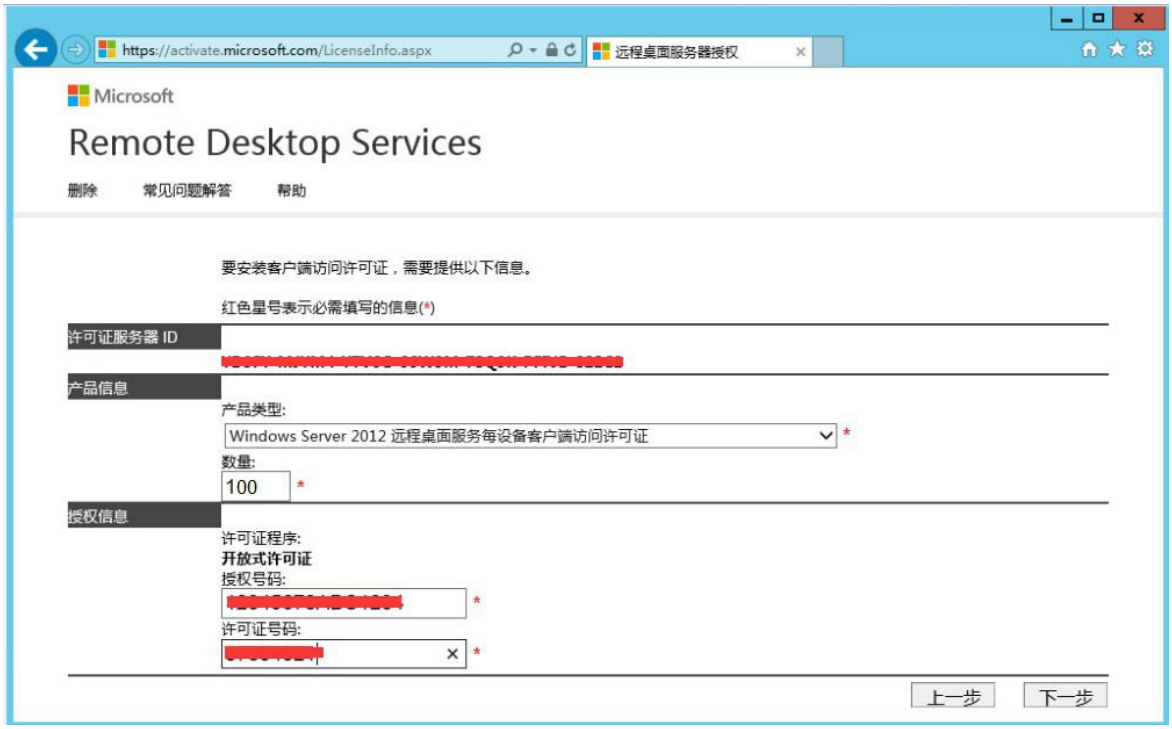
图 45 RDS 授权信息填写页面

图 44 安装客户端许可


https://activate.microsoft.com/
远程桌面服务器授权
Microsoft
Remote Desktop Services
删除
常见问题解答
帮助
要安装许可证，需要提供以下信息。通过选择“远程桌面授权管理器”工具中的“安装许可证”可以找到许可证服务器 ID。连接方法应设置为 Web 浏览器 (Windows Server 2008) 或 Web 浏览器 (Windows Server 2003)。要更改连接方法，请在“远程桌面授权管理器”工具的“视图”菜单上单击“属性”，然后单击“连接方法”选项卡。
红色星号表示必需填写的信息 (*).
产品信息
许可证服务器 ID
授权信息
许可证程序:
开放式许可证
公司信息
公司:
test
国家(地区):
中国
上一步
下一步

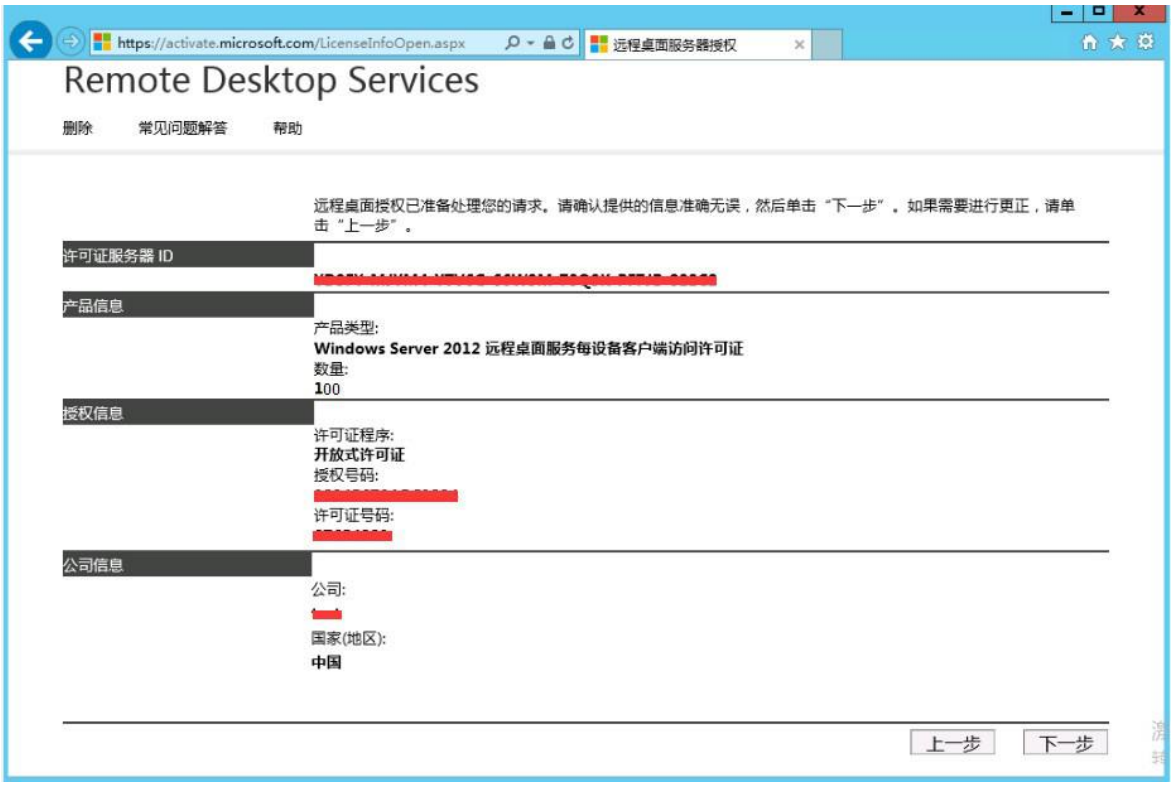
步骤 17 单击<下一步>进入 RDS 授权许可证填写页面：选择“windows server 2012 远程桌面服务每设备客户端访问许可证”，填写正确的许可证号码的数量，填写微软授权正确的授权号码。

图 46 RDS 授权许可证填写页面

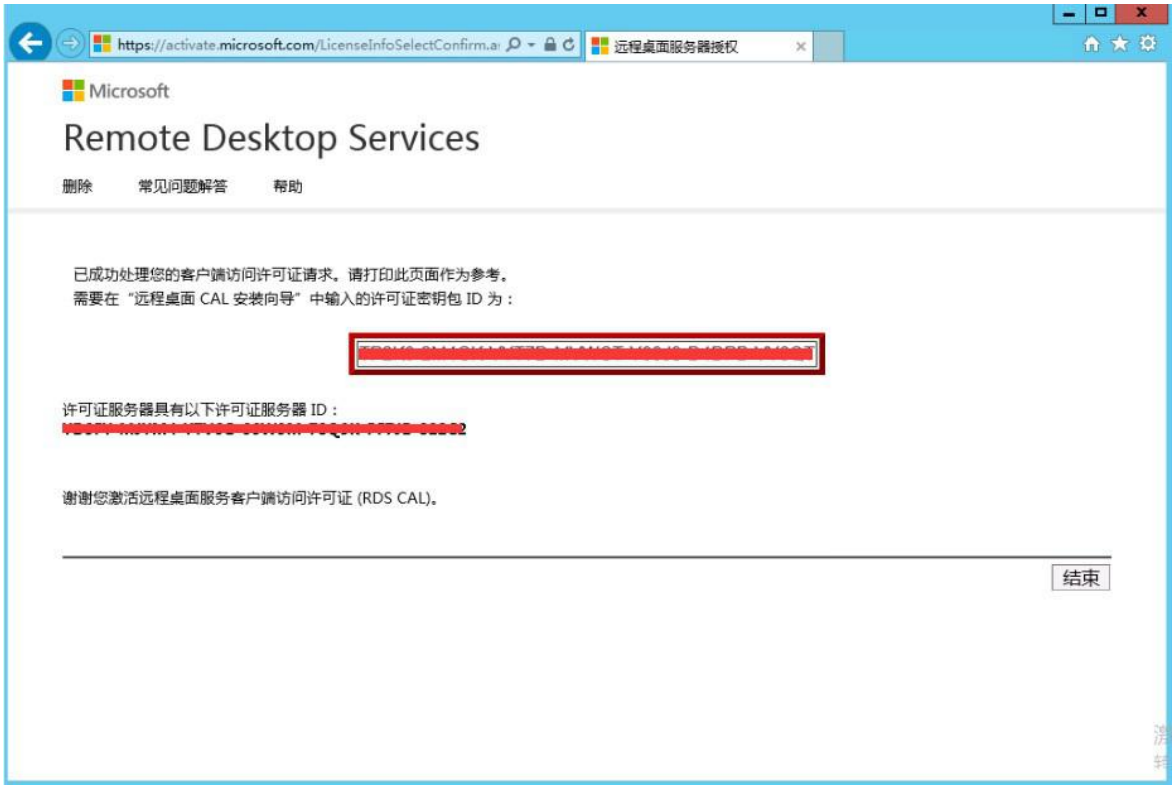


步骤 18 单击<下一步>进入 RDS 授权信息确认页面。

图 47 RDS 授权信息确

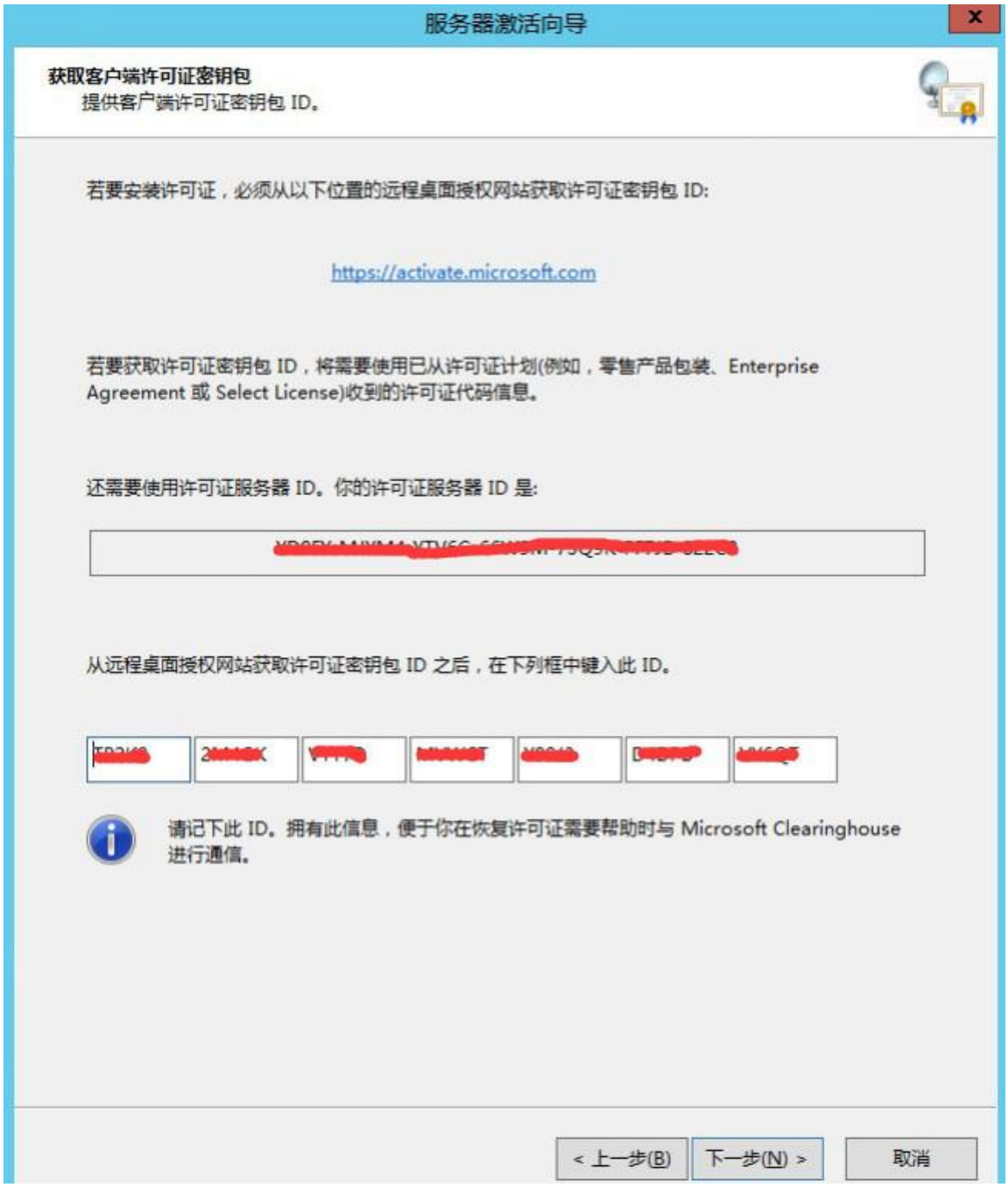


步骤 19 单击<下一步>RDS 授权一个许可证密钥包 ID 号，将其复制并保存好。

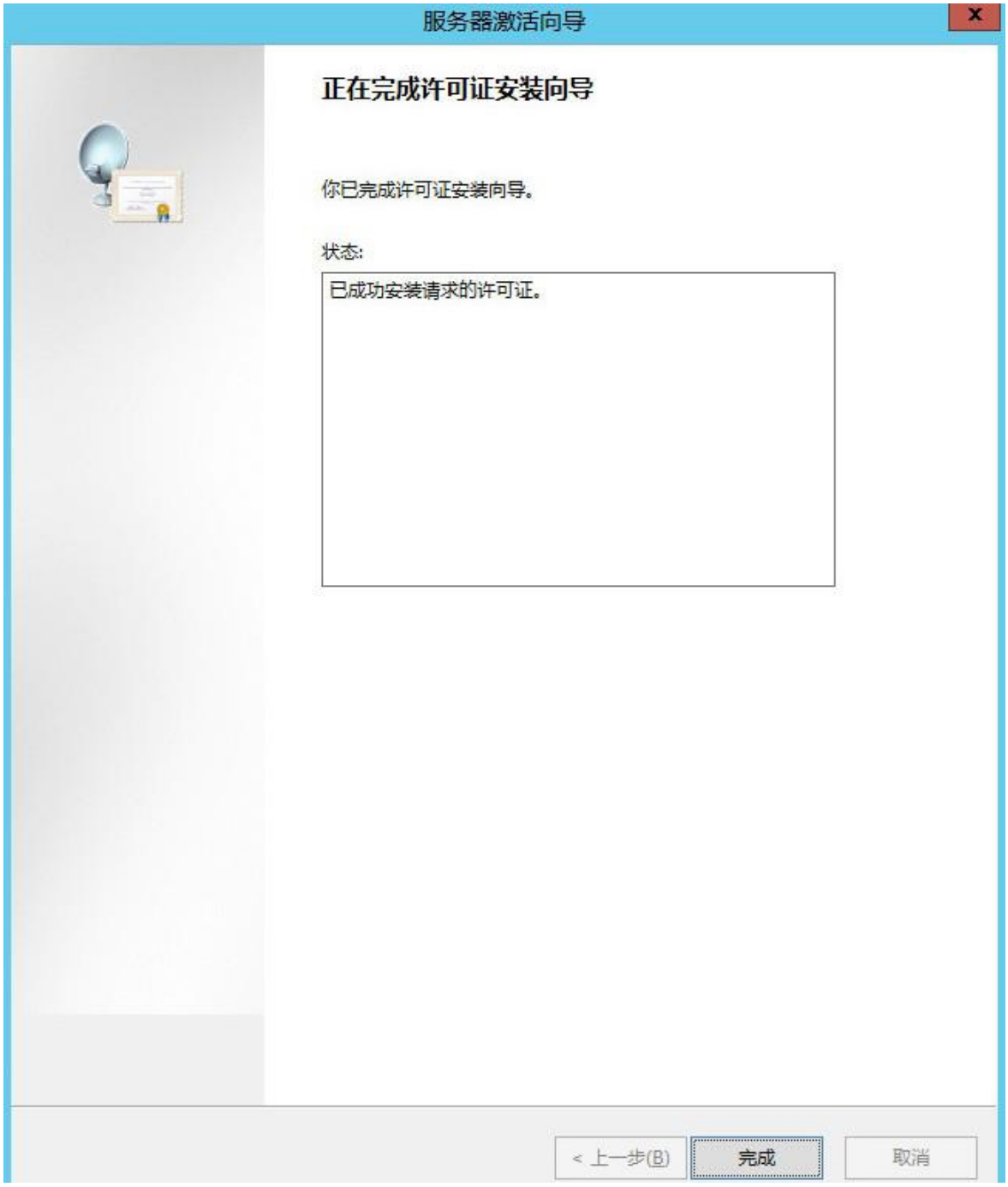


步骤 20 返回获取客户端许可证密钥包界面，填写正确的许可证密钥包 ID 号。

图 49 填写正确的许可证密钥包



步骤 21 单击<下一步>进入正在完成许可证安装向导界面。



步骤 22 单击<完成>后，可以在 RD 授权管理器窗口中看到已进行了授权。

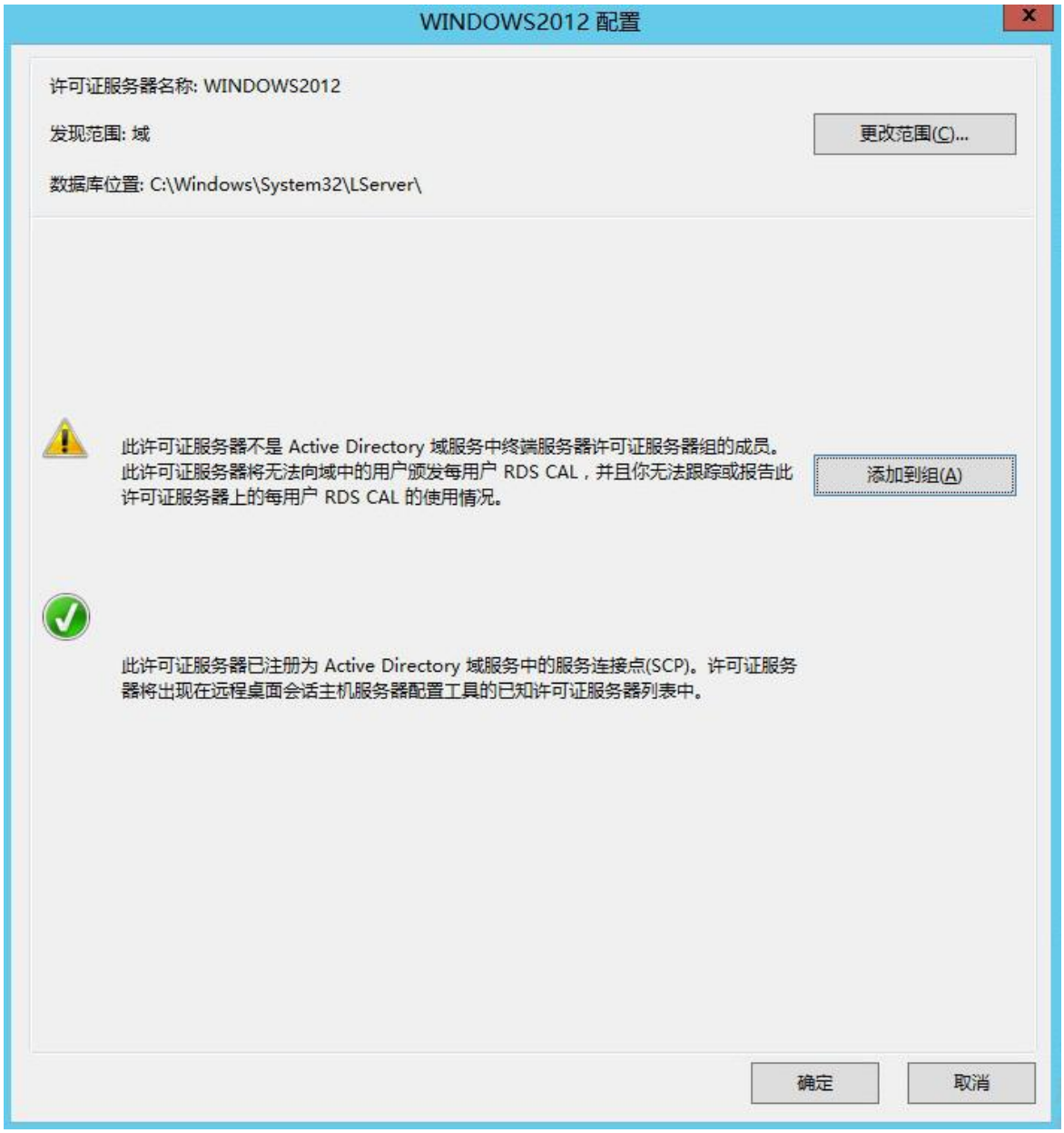
图 51 RD 授权管理

步骤 23 右击计算机名称，选择“复查配置”。

图 52 复查配置界面

步骤 24 单击<复查配置>进入配置界面。

图 53 Windows2012 配

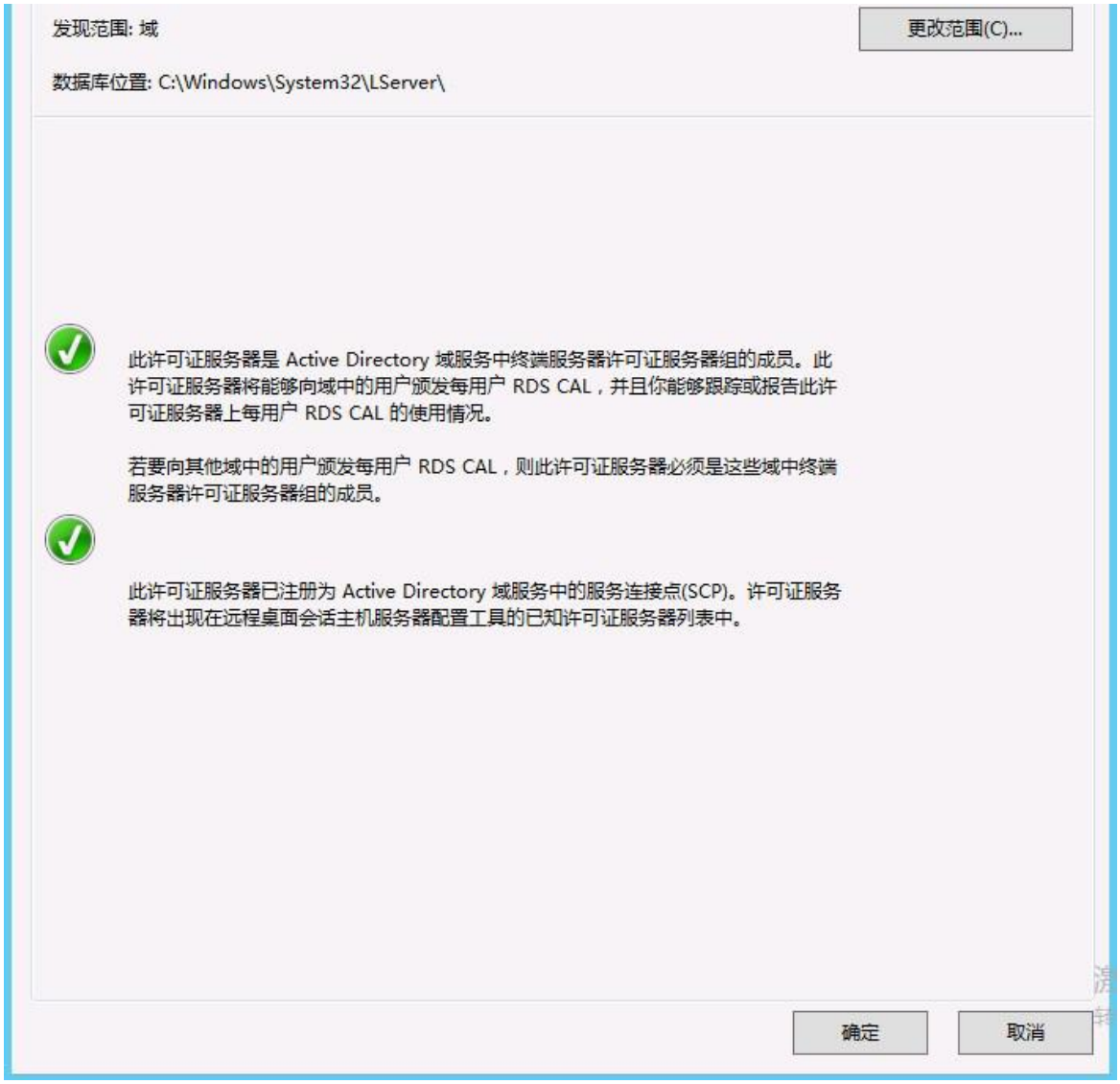


步骤 25 单击<添加到组>后弹出 RD 授权管理器窗口。

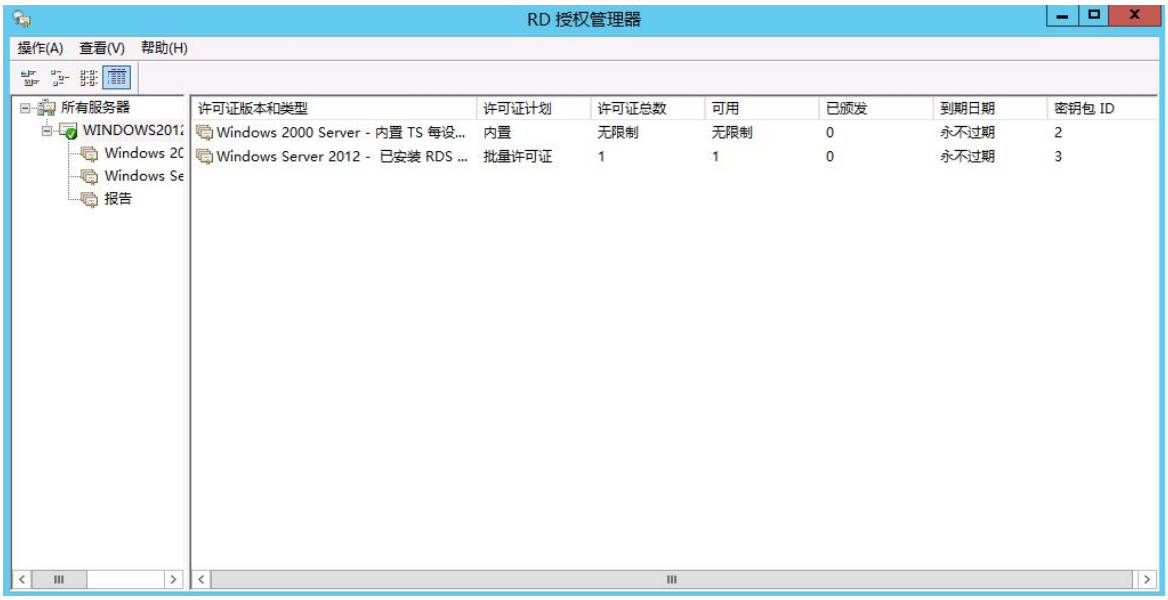
步骤 26 单击<确定>后即可成功。

图 55 确定成功

图 54 RD 授权管理



步骤 27 单击<确定>后，在 RD 授权管理器中可以看到打上了绿色的勾勾。

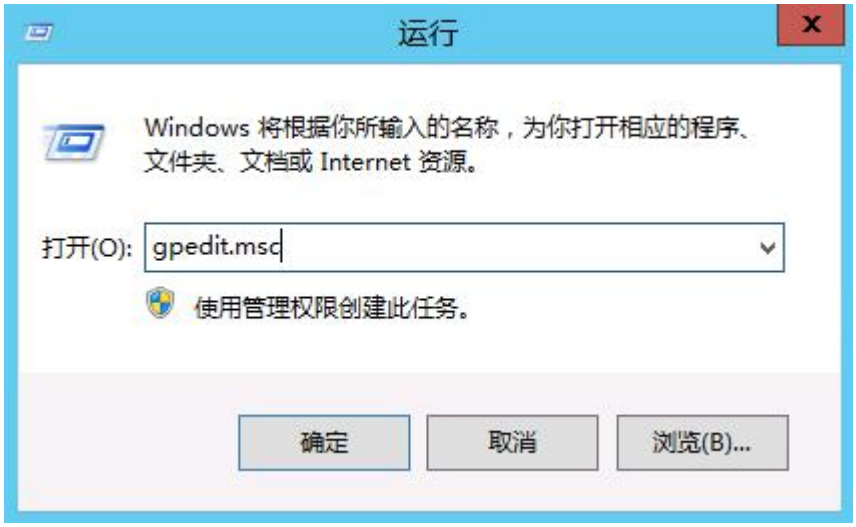


7.2.4 调整本地组策略

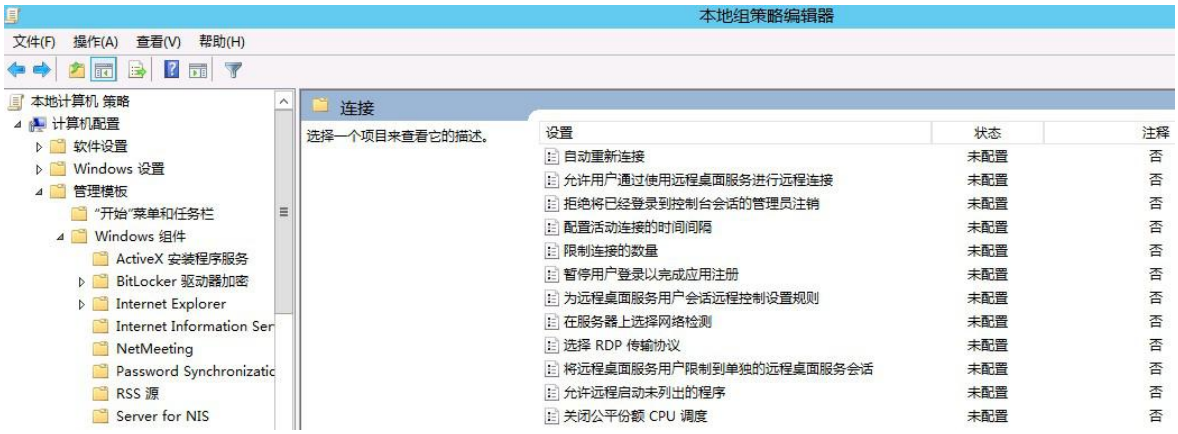
步骤 1 在系统的运行窗口中，输入“gpedit.msc”。

图 57 运行窗口

图 56 RD 授权管理



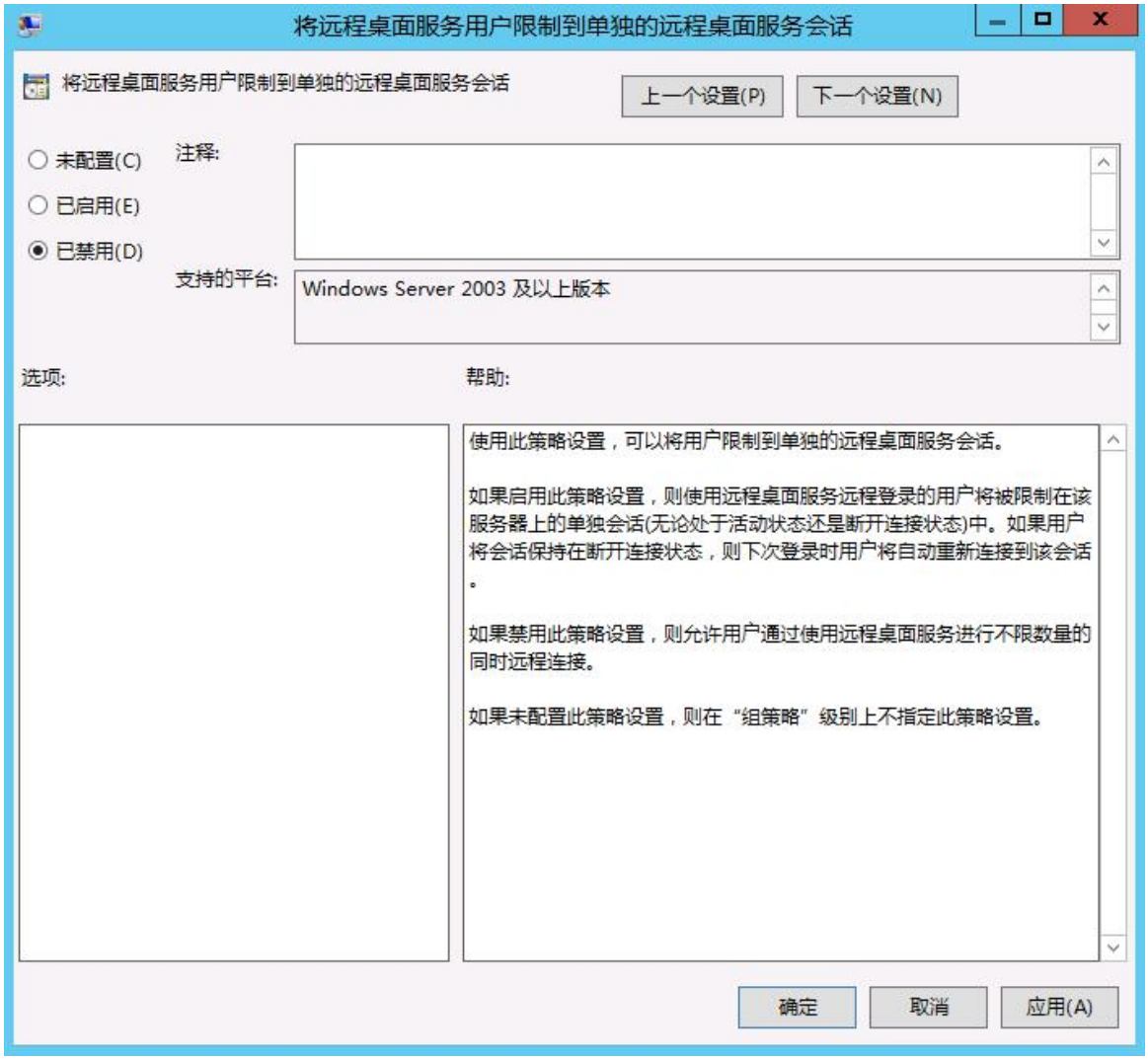
步骤 2 单击<确定>进入[计算机配置/管理模板/windows 组件/远程桌面服务/远程桌面会话主机/连接]界面。



步骤 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>，在配置界面中设置为“已禁用”。

图 59 将远程桌面服务用户限制到单独的远程桌面服务会话界面

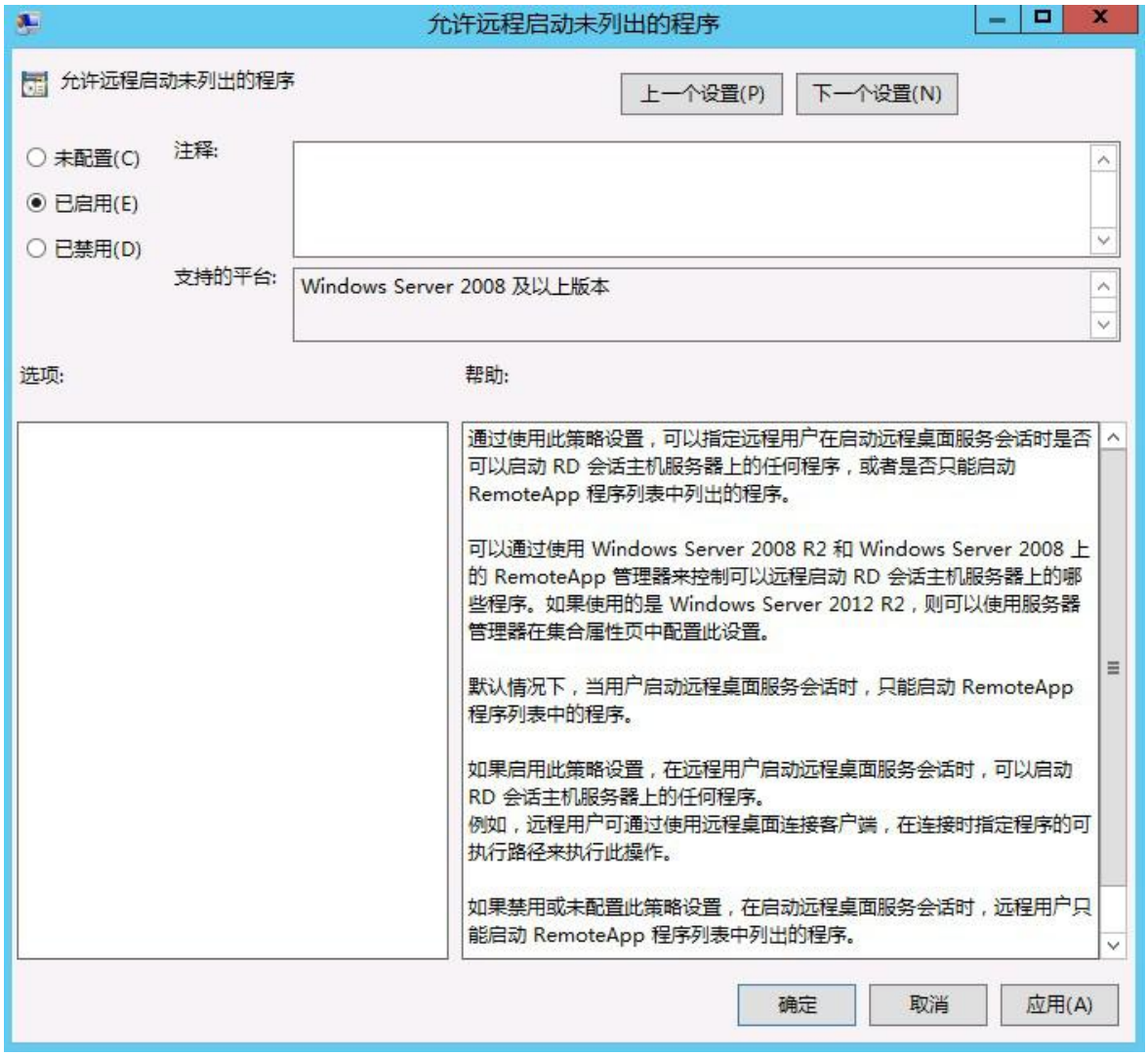
图 58 本地组策略编辑


将远程桌面服务用户限制到单独的远程桌面服务会话
将远程桌面服务用户限制到单独的远程桌面服务会话
上一个设置(P)
下一个设置(N)
未配置(C)
已启用(E)
已禁用(D)
注释:
支持的平台:
Windows Server 2003 及以上版本
选项:
帮助:
使用此策略设置，可以将用户限制到单独的远程桌面服务会话。
如果启用此策略设置，则使用远程桌面服务远程登录的用户将被限制在该服务器上的单独会话(无论处于活动状态还是断开连接状态)中。如果用户将会话保持在断开连接状态，则下次登录时用户将自动重新连接到该会话。
如果禁用此策略设置，则允许用户通过使用远程桌面服务进行不限数量的同时远程连接。
如果未配置此策略设置，则在“组策略”级别上不指定此策略设置。
确定
取消
应用(A)

步骤 4 单击<确定>即可。

步骤 5 双击<允许远程启动未列出的程序>，在配置界面中选择“已启用”。

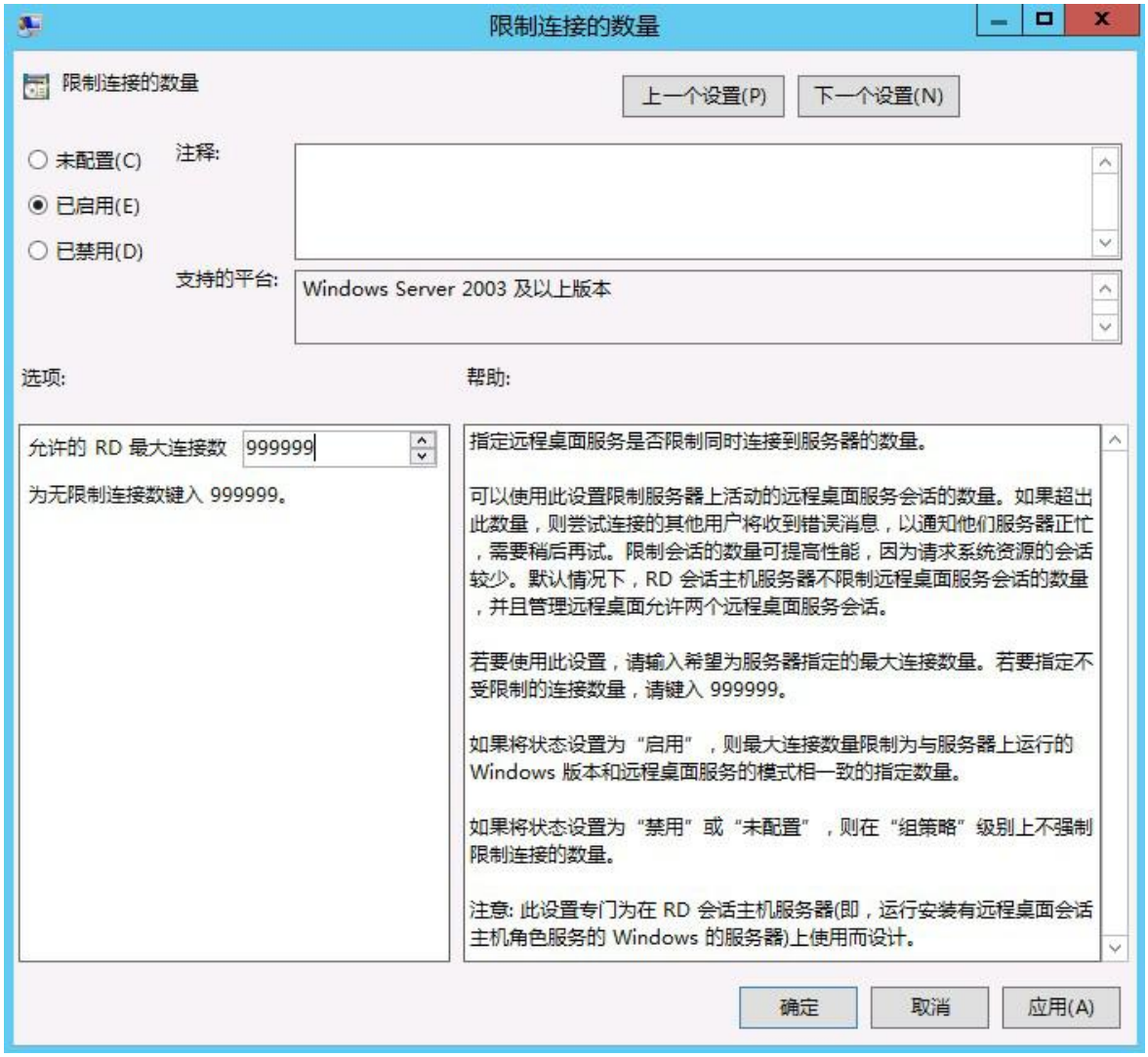
图 60 允许远程启动未列出的程序



步骤 6 单击<确定>即可。

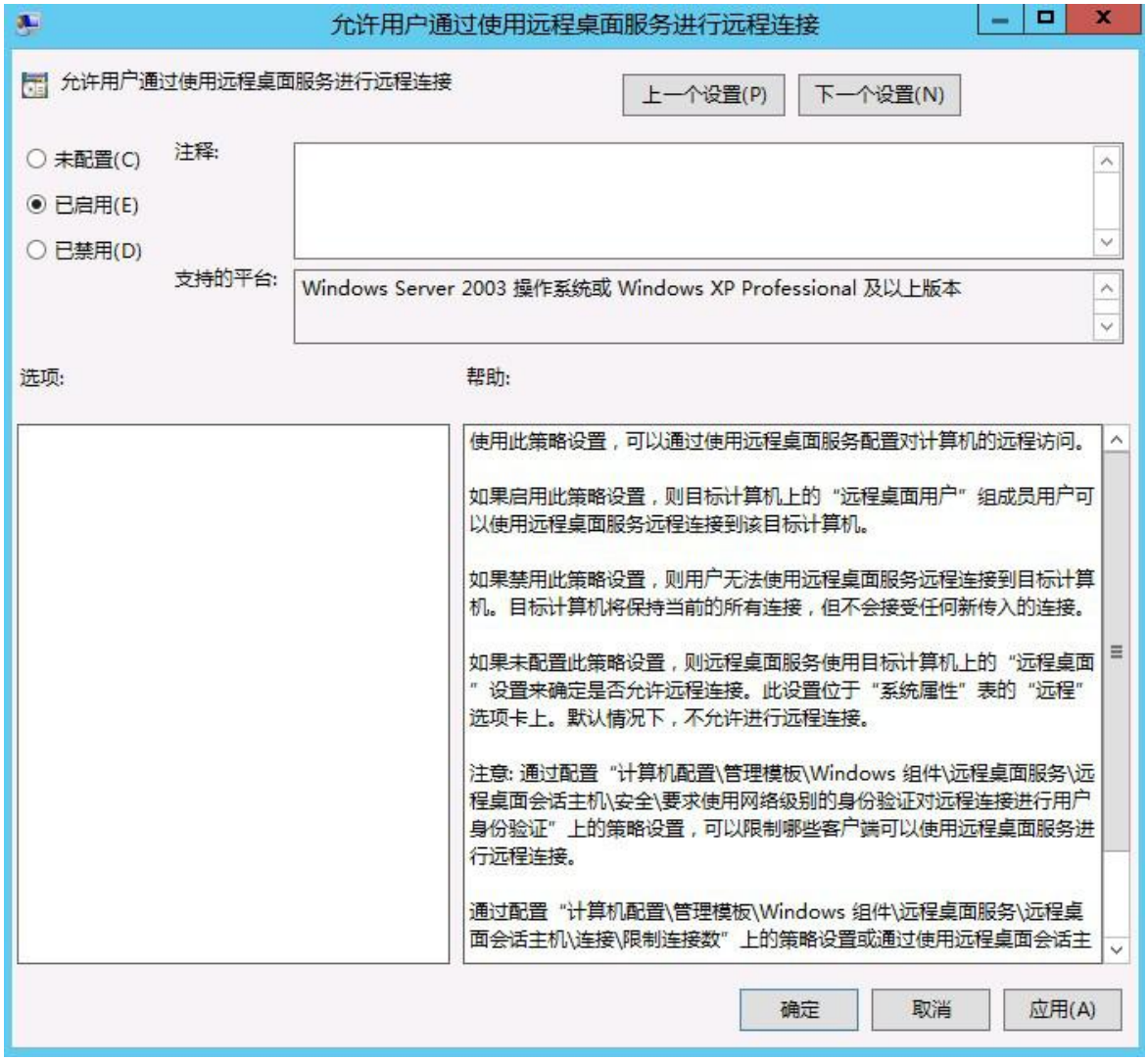
步骤 7 双击<限制连接的数量>，在配置界面中设置“已启用”，输入允许的 RD 最大连接数“999999”。

图 61 限制连接的数



步骤 8 单击<确定>后即可。

步骤 9 双击<允许用户通过远程桌面服务进行远程连接>，在配置界面中选择“已启用”。



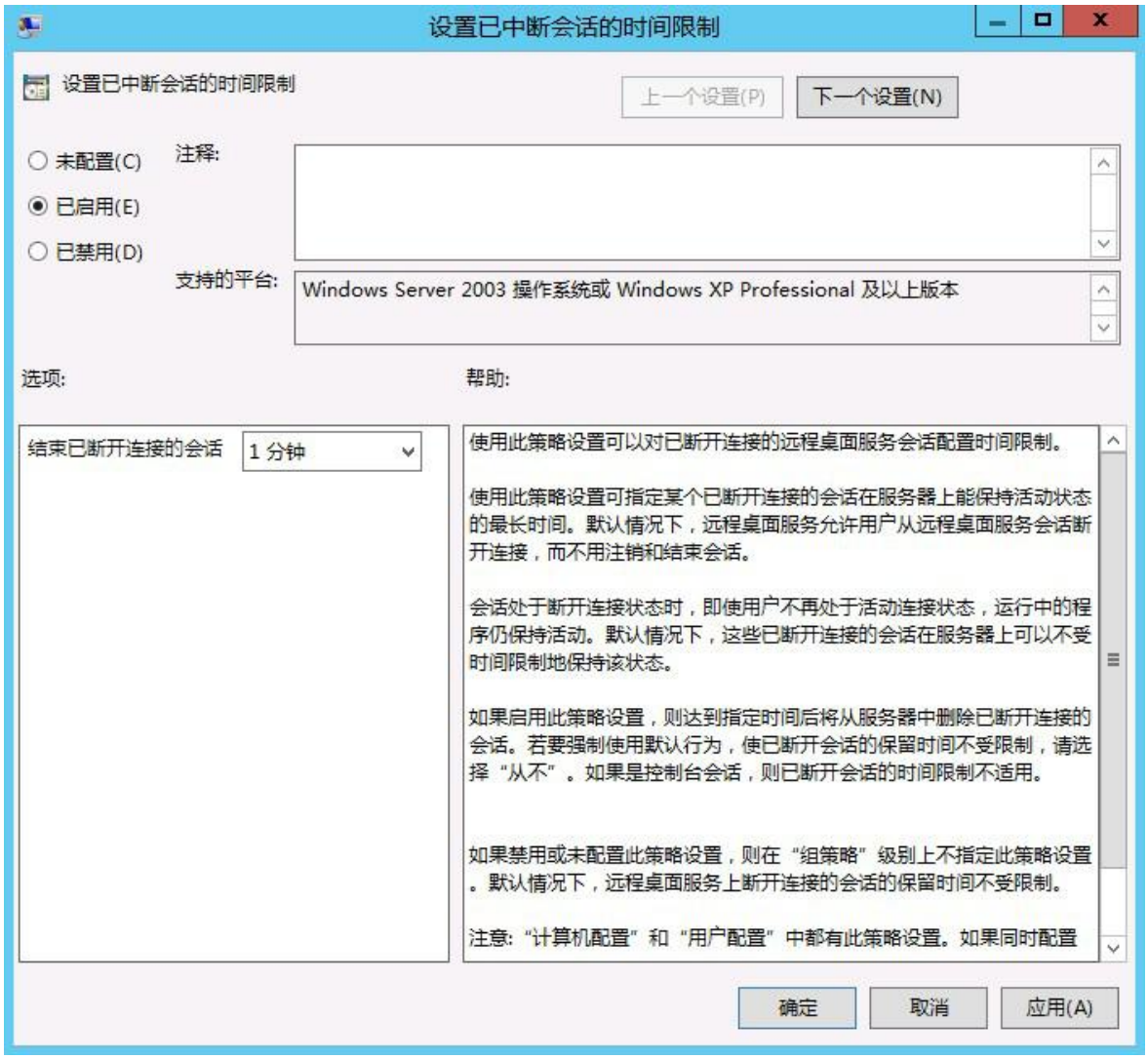
步骤 10 单击<确定>即可。

步骤 11 再进入[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 63 本地组策略编辑器

图 62 允许用户通过远程桌面服务进行远程连

步骤 12 双击<设置已中断会话的时间限制>，在配置界面中设置“已启用”，结束已断开连接的会话为“1 分钟”。

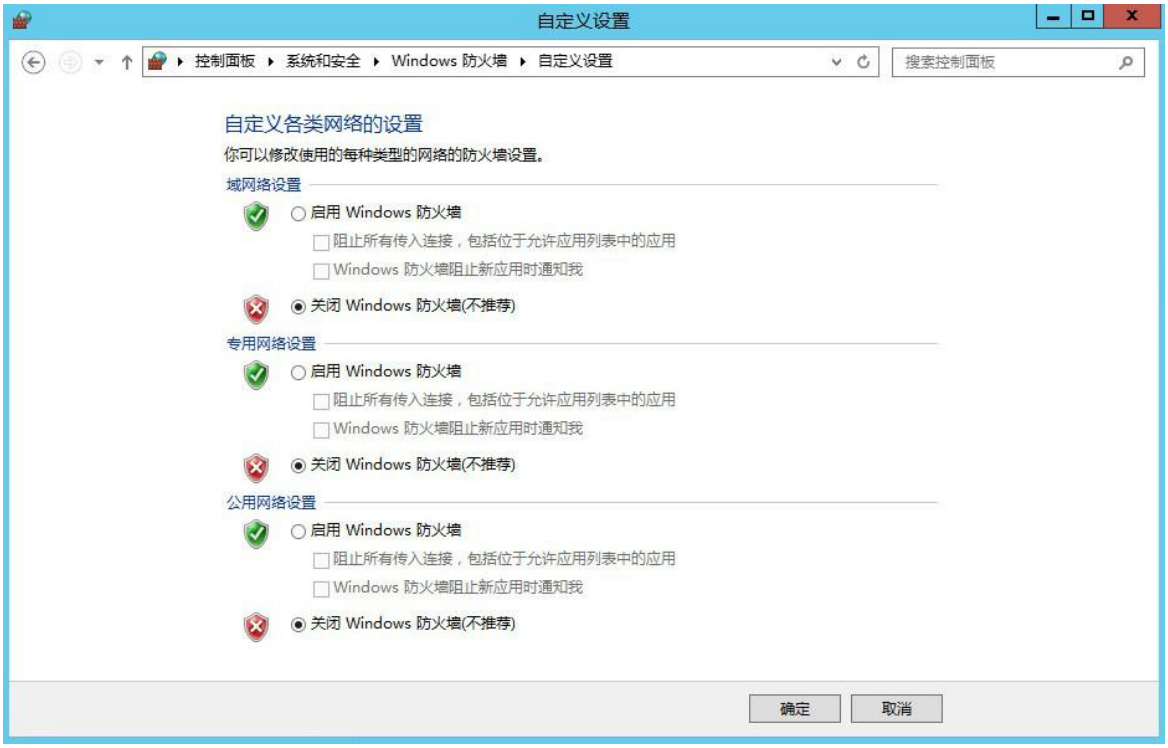

设置已中断会话的时间限制
设置已中断会话的时间限制
上一个设置(P)
下一个设置(N)
未配置(C)
已启用(E)
已禁用(D)
注释:
支持的平台:
Windows Server 2003 操作系统或 Windows XP Professional 及以上版本
选项:
帮助:
结束已断开连接的会话
1 分钟
使用此策略设置可以对已断开连接的远程桌面服务会话配置时间限制。
使用此策略设置可指定某个已断开连接的会话在服务器上能保持活动状态的最长时间。默认情况下，远程桌面服务允许用户从远程桌面服务会话断开连接，而不用注销和结束会话。
会话处于断开连接状态时，即使用户不再处于活动连接状态，运行中的程序仍保持活动。默认情况下，这些已断开连接的会话在服务器上可以不受时间限制地保持该状态。
如果启用此策略设置，则达到指定时间后将从服务器中删除已断开连接的会话。若要强制使用默认行为，使已断开会话的保留时间不受限制，请选择“从不”。如果是控制台会话，则已断开会话的时间限制不适用。
如果禁用或未配置此策略设置，则在“组策略”级别上不指定此策略设置。默认情况下，远程桌面服务上断开连接的会话的保留时间不受限制。
注意：“计算机配置”和“用户配置”中都有此策略设置。如果同时配置
确定
取消
应用(A)

步骤 13 单击<确定>即可。

图 64 设置已中断会话的时

7.2.5 关闭 Windows 防火墙

步骤 1 进入[控制面板/系统和安全/windows 防火墙/自定义设置]界面中，将防火墙关闭。



步骤 2 单击<确定>即可。

7.2.6 关闭 IE 增强的安全配置

步骤 1 进入[服务器管理器/本地服务器]界面中，找到右侧的“IE 增强的安全配置”。

图 66 服务器管理器

图 65 自 定

步骤 2 单击<启用>进入 IE 增强的安全配置界面，选择“关闭”。


Internet Explorer 增强的安全配置
Internet Explorer 增强的安全配置(IE ESC)降低了你的服务器暴露于来自基于 Web 内容的潜在攻击的风险。
Internet Explorer 增强的安全配置默认情况下为 Administrators 组和 Users 组启用。
管理员(A):
启用(推荐)
关闭
用户(U):
启用(推荐)
关闭
有关 Internet Explorer 增强的安全配置的详细信息
确定
取消

步骤 3 单击<确定>即可。

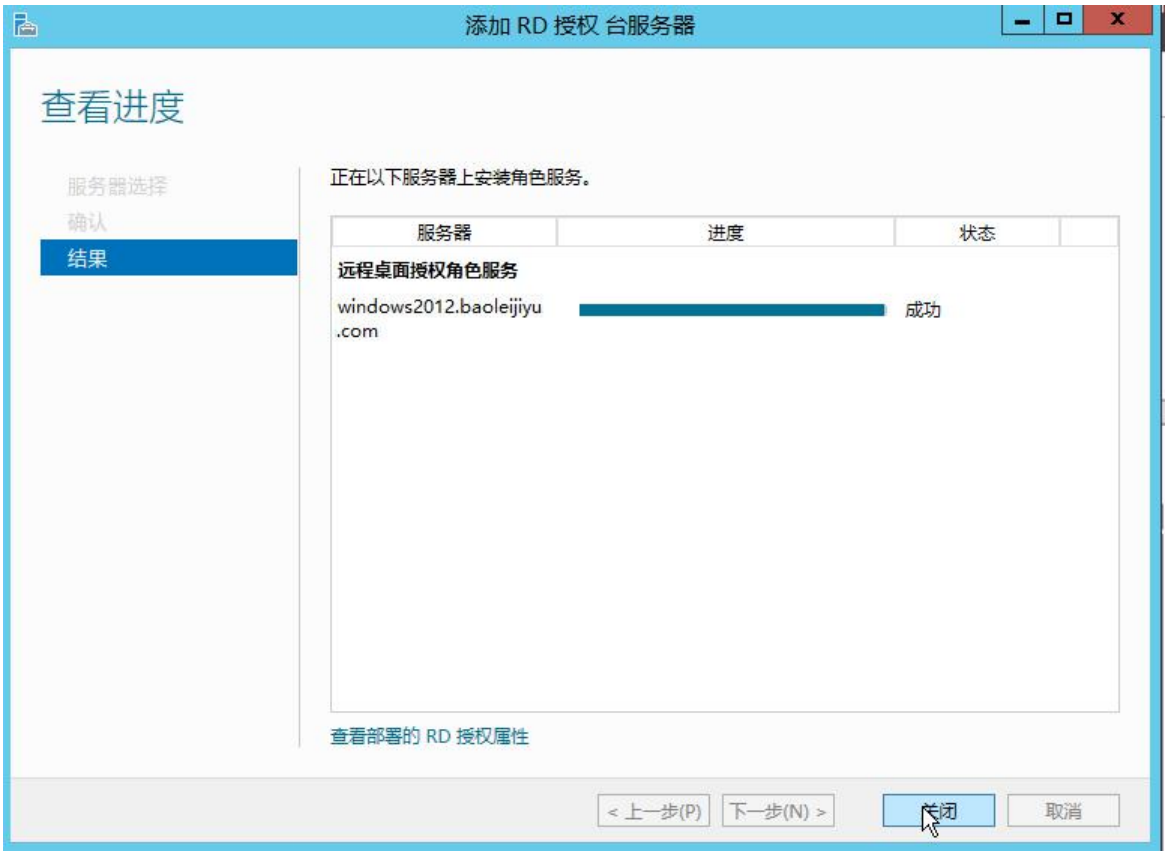
图 67 IE 增强的安全配

7.2.7 添加 RD 授权

步骤 1 进入[服务器管理器/远程桌面服务/概述]界面。

步骤 2 在部署概述界面中，选择“RD 授权”图标添加 RD 授权服务器，将本机添加到 RD 授权服务器中。

图 69 服务器管理器-RD



7.2.8 设置 RD 授权模式

步骤 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 70 远程桌面服务界面

步骤 2 双击<RD 授权诊断程序>进入界面，看到“RD 授权诊断程序信息-警告”中有警告信息，表示 RD 授权未配置完成。

图 71 RD 授权诊

步骤 3 进入[服务器管理器/远程桌面服务/概述]界面。

图 72 服务器管理器


服务器管理器
服务器管理器 ▸ 远程桌面服务 ▸ 概述
管理(M) 工具(T) 视图(V) 帮助(H)
概述
服务器
集合
QuickSessionC...
开始使用远程桌面服务
1 设置远程桌面服务部署
快速启动
基于虚拟机的桌面部署
2 添加 RD 虚拟化主机服务器
3 创建虚拟机集合
基于会话的桌面
2 添加 RD 会
3 创建会话集
了解详细信息
部署概述
RD 连接代理服务器: WIN-2KTUH1CEKRS.hfnboatest.com
管理方式: HFNBOATEST\administrator
任务
编辑部署属性(E)
连接到其他部署(C)
刷新(R)
部署服务器
上次刷新时间 2019/8/2
服务器 FQDN
WIN-2KTUH1CEKRS.
WIN-2KTUH1CEKRS.
WIN-2KTUH1CEKRS.
WIN-2KTUH1CEKRS.
RD Web 访问
RD 网关
RD 授权
RD 连接代理

步骤 4 单击<任务>中的<编辑部署属性>进入部署属性界面，在 RD 授权界面中，选择“每设备”、添加“计算机名域名”。

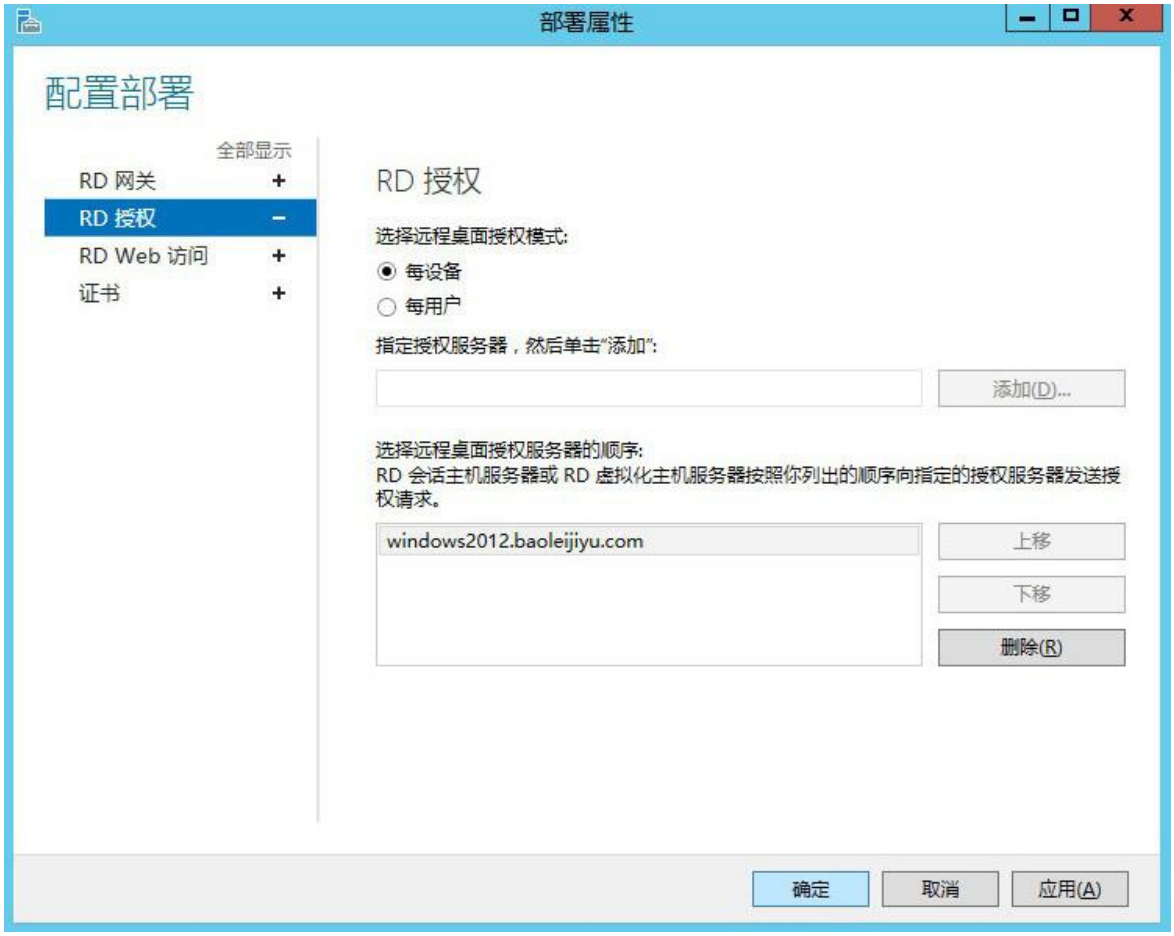
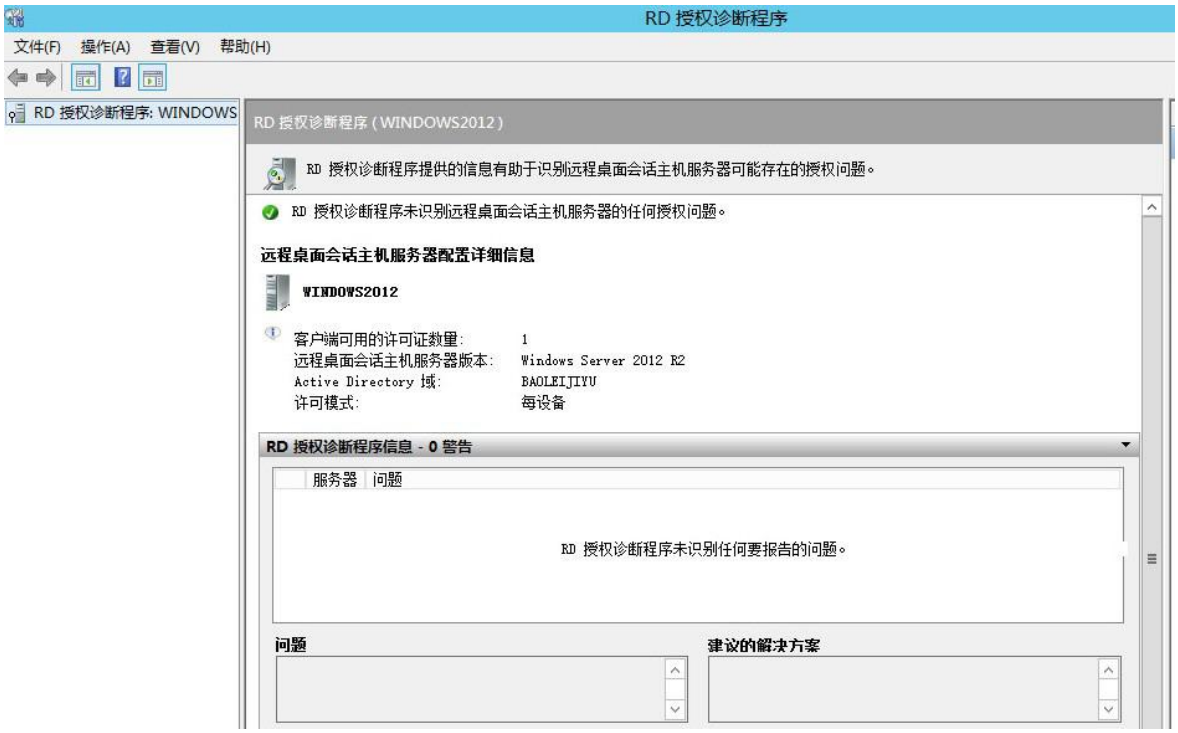


图 73 编辑部署属性

步骤 5 单击<确定>后即可。

步骤 6 返回 RD 授权诊断程序界面，可以看到警告信息已为空，表示 RD 授权正常。



7.2.9 开启远程桌面

步骤 1 右击计算机，单击<属性>进入系统属性界面。

图 75 系统属

步骤 2 单击<远程设置>进入远程桌面配置窗口，选择“允许连接到此计算机”，取消“仅允许运行使用网络级别身份验证的远程桌面的计算机连接(建议)”。

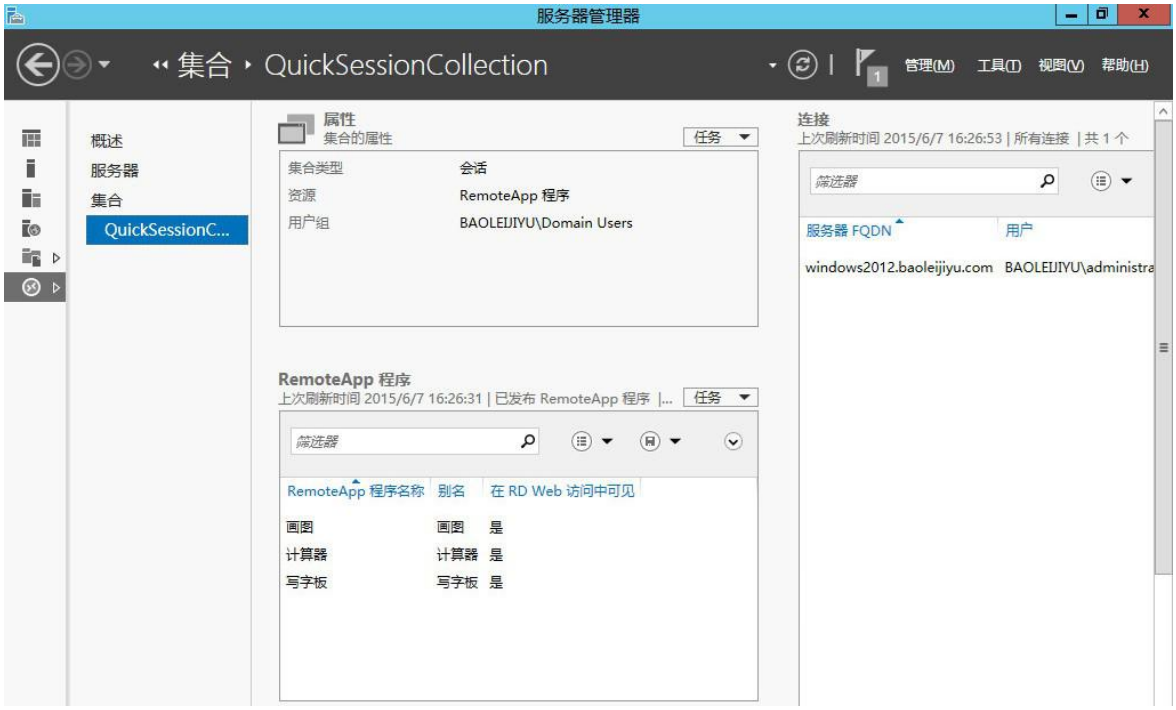

系统属性
计算机名
硬件
高级
远程
远程协助
允许远程协助连接这台计算机(R)
高级(V)...
远程桌面
选择一个选项，然后指定谁可以连接。
不允许远程连接到此计算机(D)
允许远程连接到此计算机(L)
仅允许运行使用网络级别身份验证的远程桌面的计算机连接(建议)(N)
帮助我选择
选择用户(S)...
确定
取消
应用(A)

步骤 3 单击<确定>即可。

图 76 远程桌面配

7.2.10 发布 RemoteApp 程序

步骤 1 进入[服务器管理器/远程桌面服务/集合/QuickSessionCollection]界面。

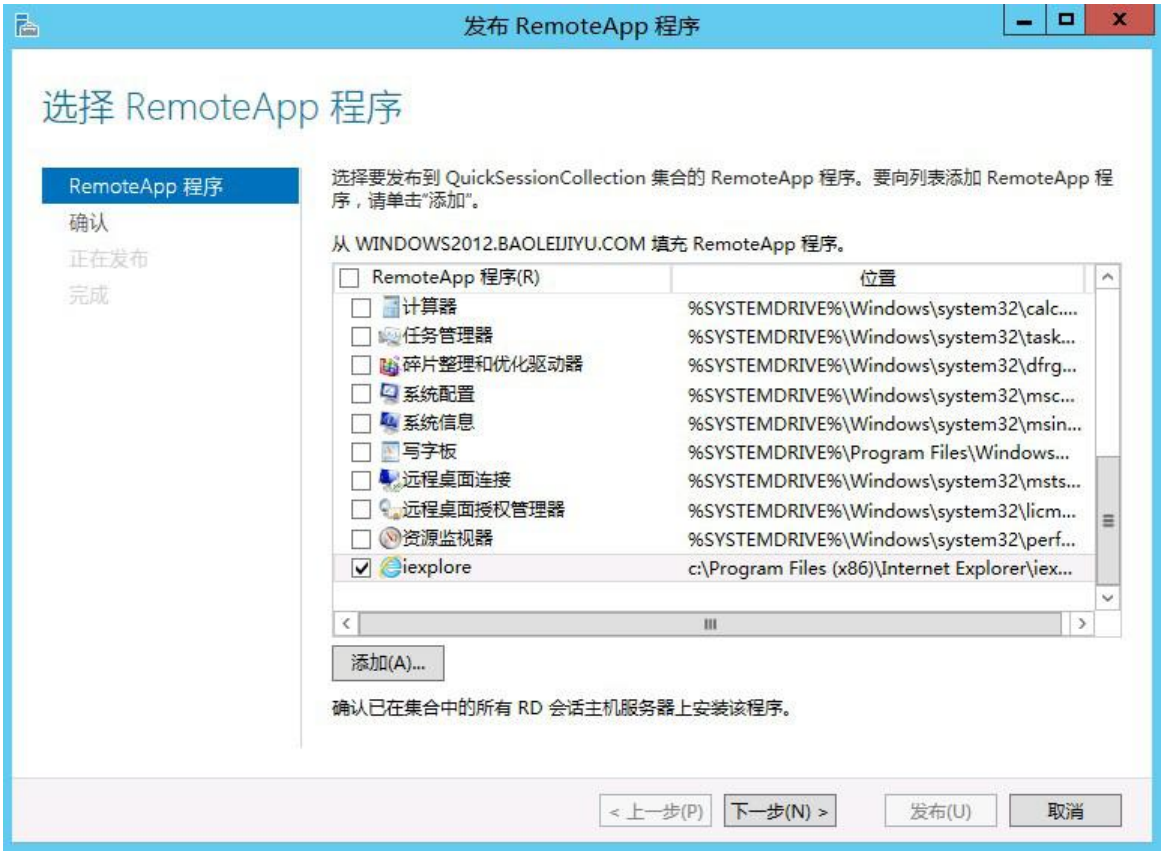


步骤 2 单击<任务>。

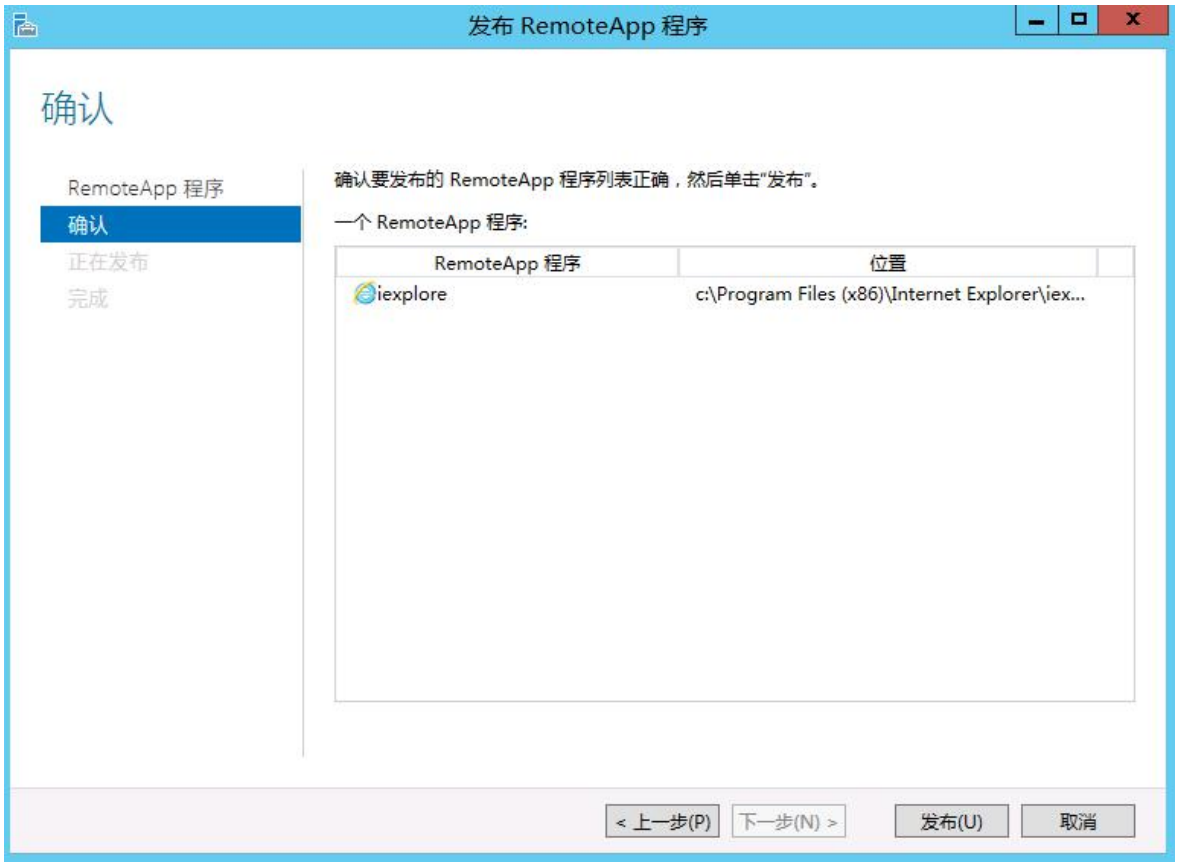
图 78 任务界面

步骤 3 单击<发布 RemoteApp 程序>进入选择 RemoteApp 程序界面，选择需要发布的应用程序。

图 79 RemoteApp 程

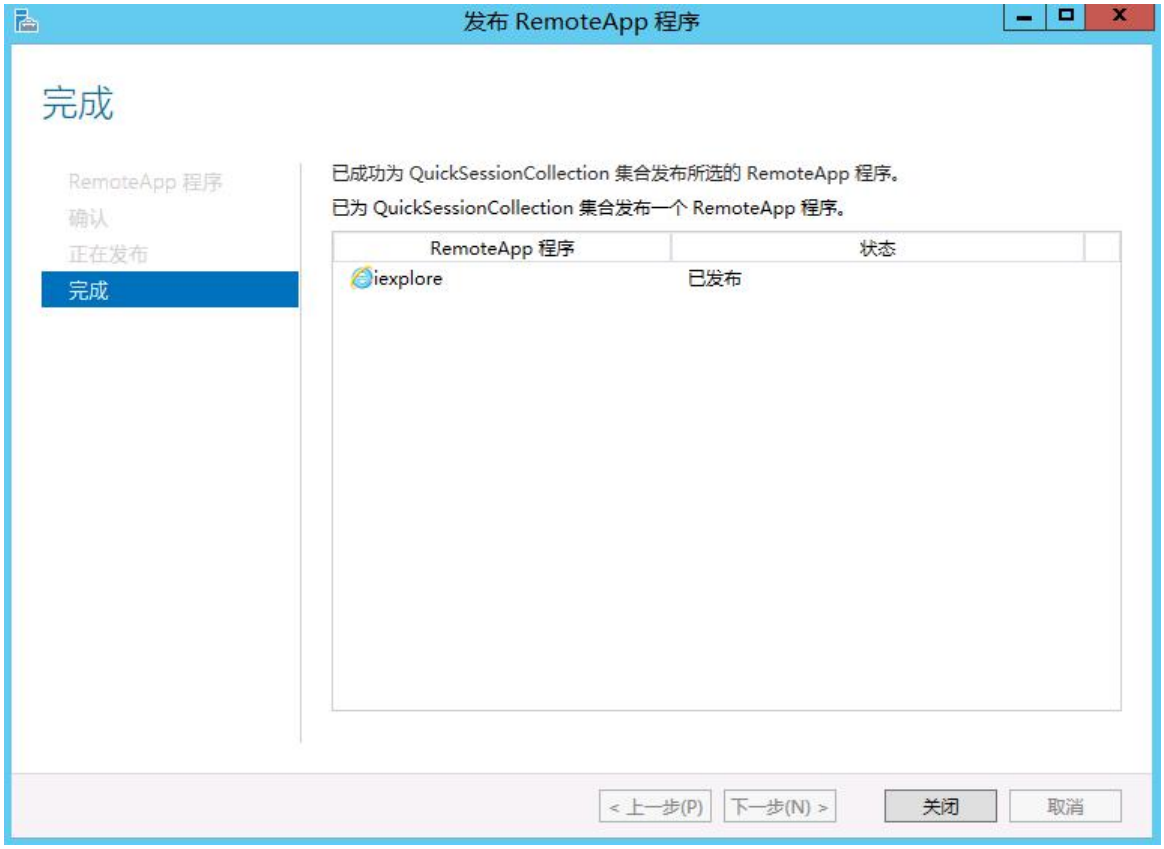


步骤 4 单击<下一步>进入确认界面。



步骤 5 单击<发布>进入发布完成界面。

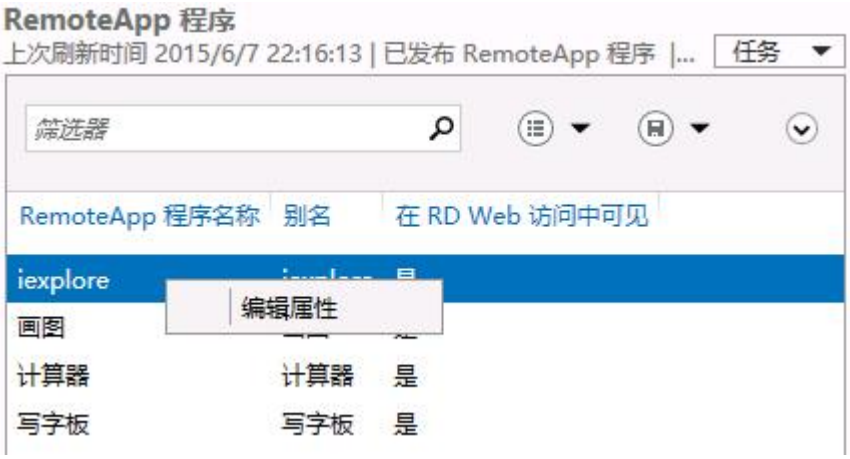
图 81 发布完



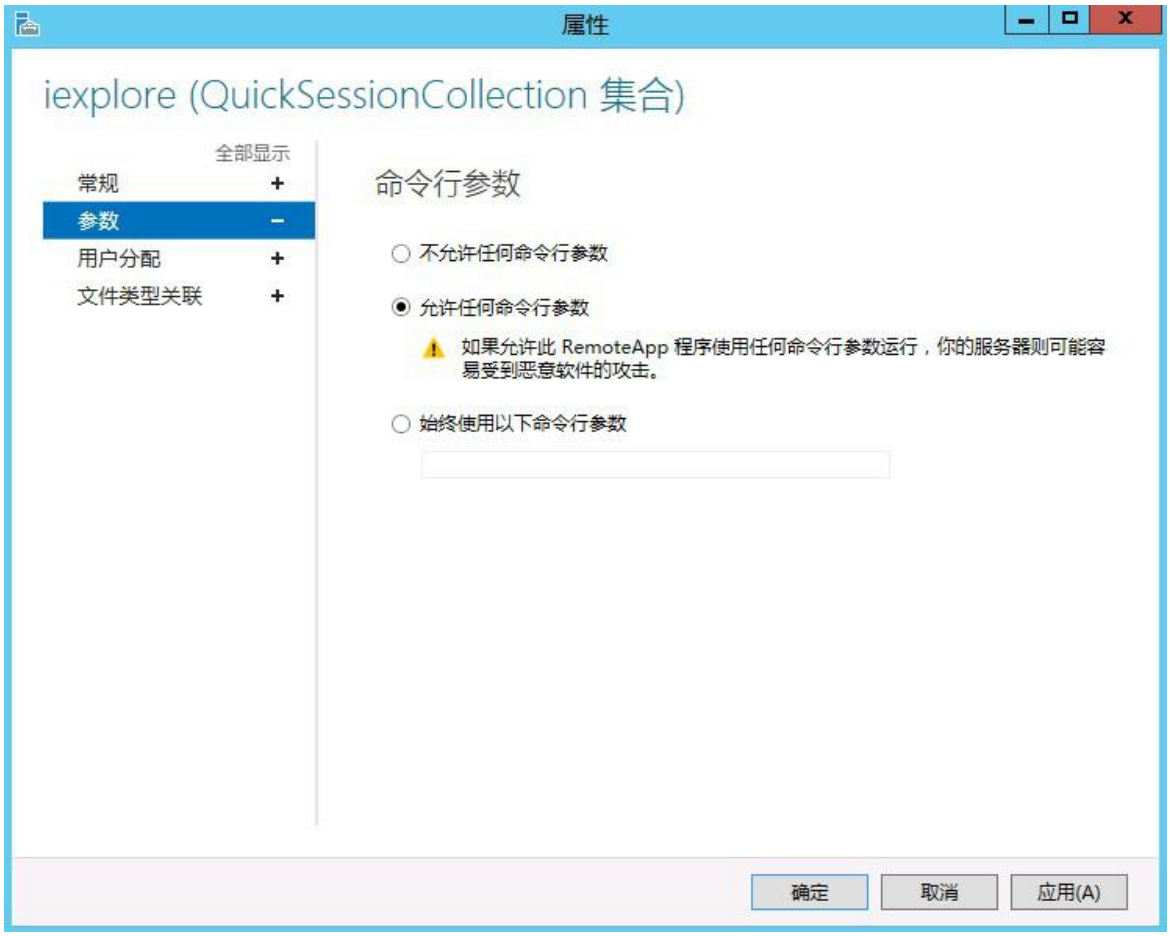
步骤 6 单击<关闭>即可。

步骤 7 右击已发布的应用程序。

图 82 已发布的应用程序界面



步骤 8 单击<编辑属性>进入应用程序的属性界面，在“参数”中选择“允许任何命令行参数”。



步骤 9 单击<确定>即可。

步骤 10 在可以访问 windows server 2012 的电脑中，请使用浏览器登录 https://应用服务器的IP/RDWeb， 并输入正确的域帐户和密码。

步骤 11 登录成功后可以看到已发布的 RemoteApp 程序。

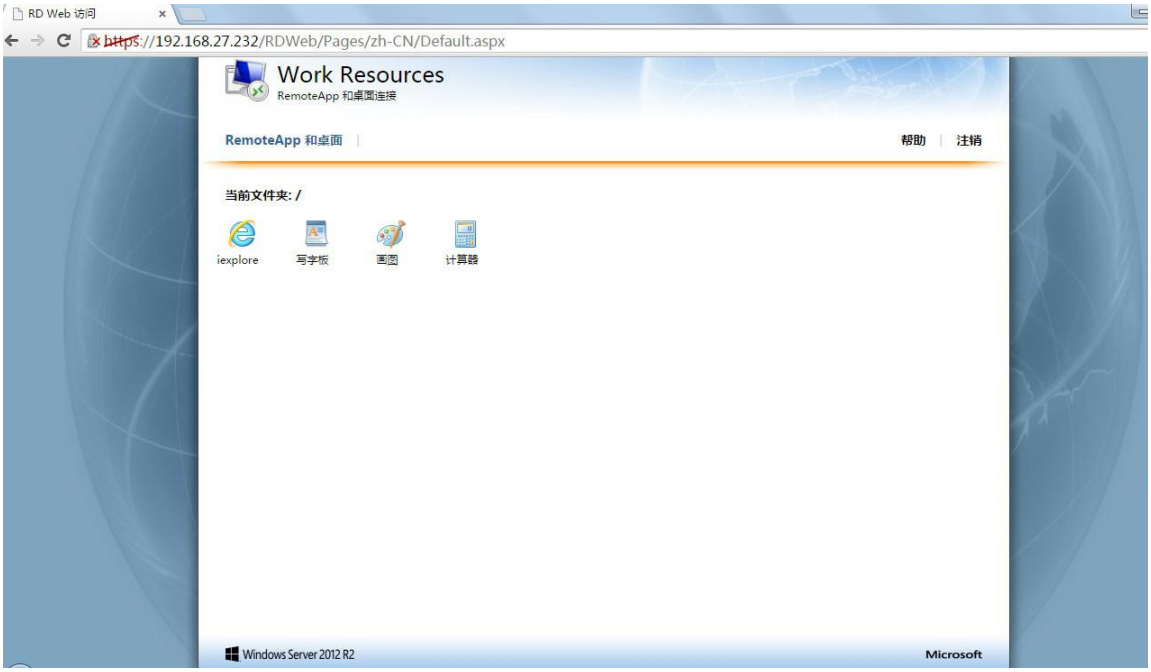


图 85 已发布的 RemoteApp 程序界面

7.3. 如何生成应用

部署应用发布的服务器已经安装好 IIS 及远程桌面服务。其中 IIS 中要包含 ASP 选项。

(wwwroot)应用发布 web 服务，将此文件夹内容拷贝到 c 盘：inetpub\wwwroot 目录下，进行 web 发布。

(apptools)将此文件拷贝到任意目录，并将文件夹内的 RemoteApp Tool.exe 右键发送到桌面快捷方式。

通过桌面快捷方式打开 RDP 制作工具，生成的 RDP 文件存放目录地址为：inetpub\wwwroot\rdp。

(setpolicy.py)修改云翼运维审计系统对应的应用发布配置及设置防火墙策略脚本。上传脚本，并将脚本更改为可执行脚本：chmod +X setpolicy.py

执行脚本：

示例：python setpolicy.py appip username pwd iconport gnic bnic bcidr

参数说明：

appip：应用发布服务器 IP 地址

username：应用发布服务器登录用户名

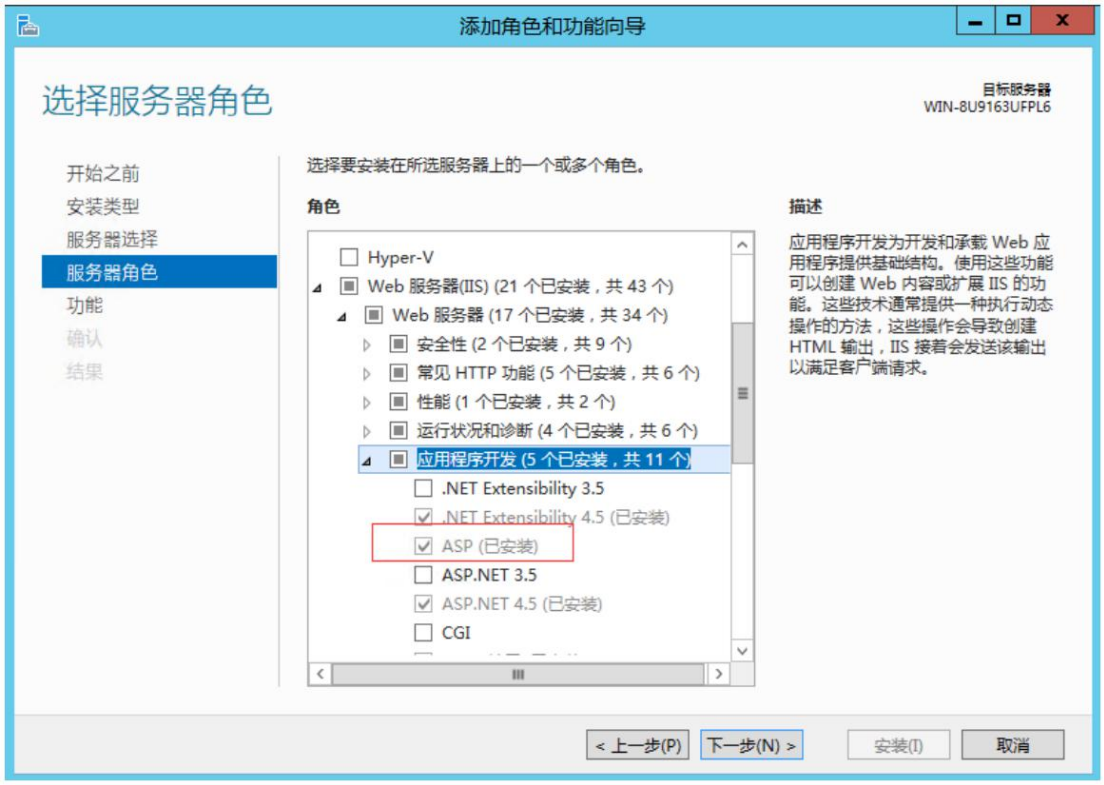
pwd：应用发布服务器登录密码，通过上述密码加密生成器，转换后的密文

iconport：自定义没有被占用的端口号，用来配置 NAT 映射获取 RDP 文件图标

gnic：云翼运维审计系统管理网卡名称，示例：ens160

bnic：云翼运维审计系统业务网卡名称，与应用发布服务器互通，示例：ens224

bcidr：业务网段 CIDR，示例：1.1.1.1/24

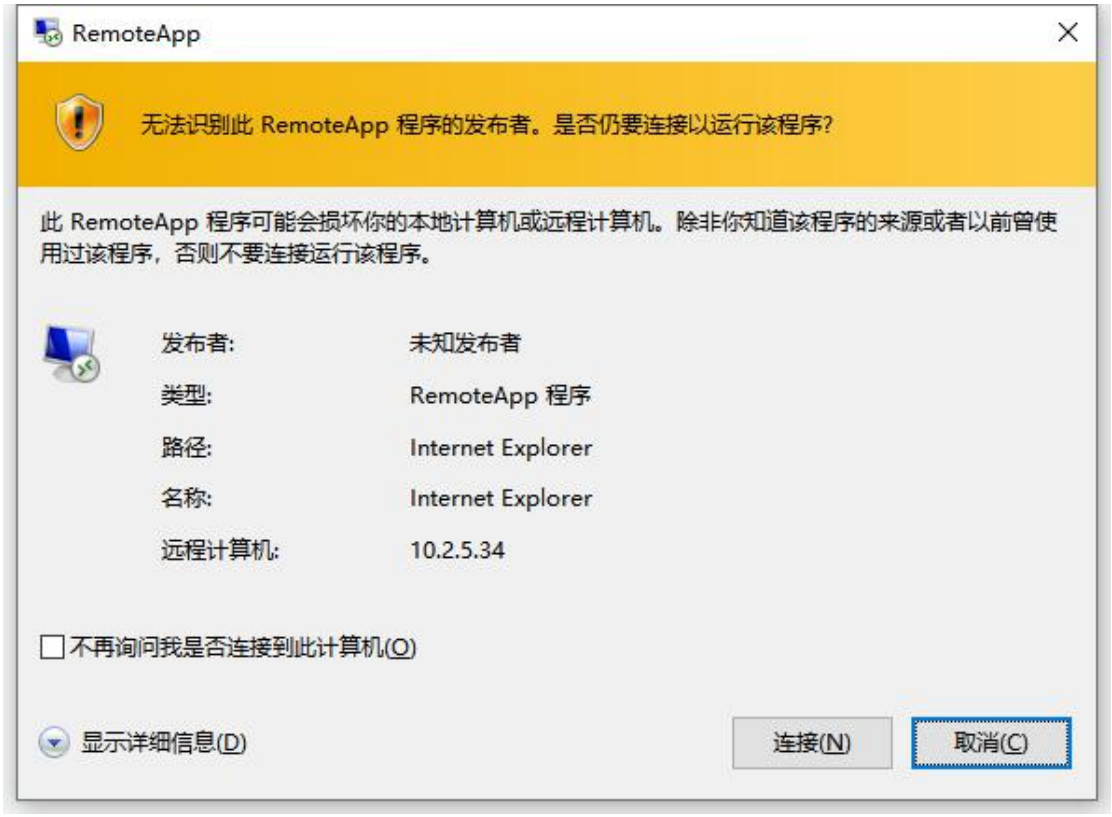


（RDP.exe）密码加密生成器，将部署应用发布工具的服务器的密码通过加密生成器转换为 rdp 可识别密文。

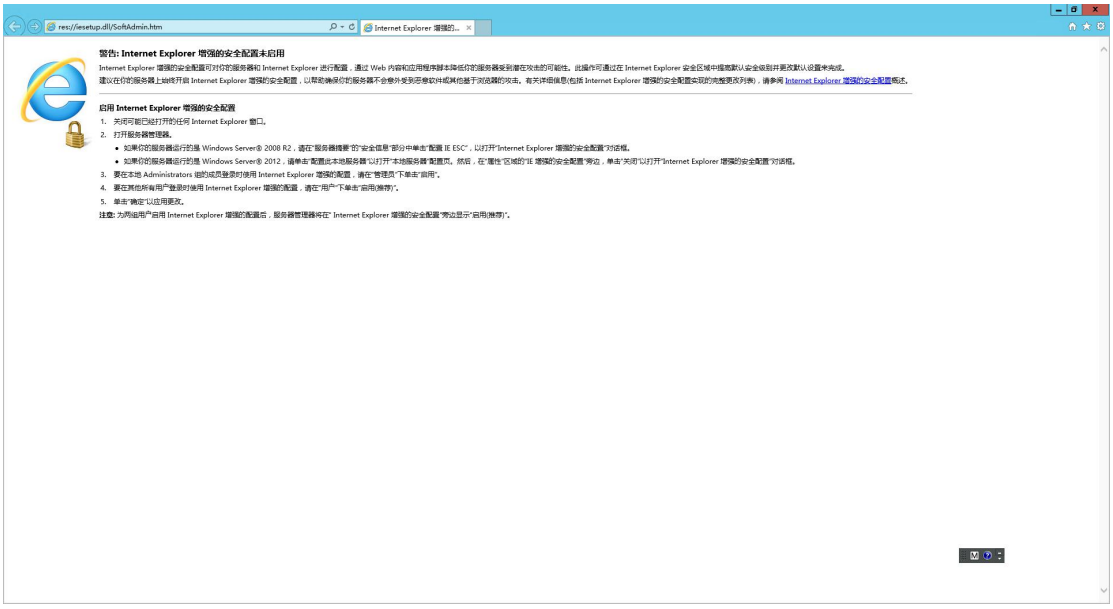
7.4. 应用发布使用方法

- 选择目标应用，点击【打开】按钮，系统会自动将文件下载至本地：

- 开发下载的.rdp 文件：



- 点击【链接】后进入自动打开应用（每个应用的操作方式相同）：



7.5. 应用分配功能

只有管理员登录可以看到应用分配功能，此功能可以为云翼运维审计系统中已经创建的账号分类特定可以用的应用。

将左侧的账号加入到右侧，点击确定，该账号就可以使用此应用；如果想取消某个账号对于该应用的使用权限，将账号从右侧框移出到左侧框内，点击确定即可。

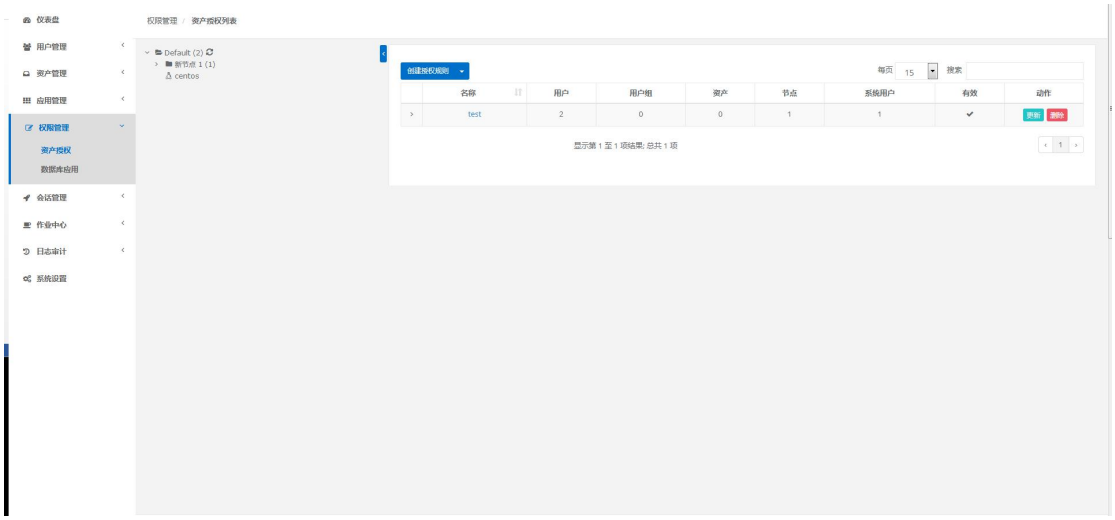
第八章. 权限管理

此功能用于将用户、系统用户和资产进行权限关联。

7.6. 资产授权

把资产授权给用户后，用户才能在 "我的资产" 里面看到资产，配置正确后用户才能正常连接资产。

7.1.1. 查看授权列表



7.1.2. 创建授权规则

进入[权限管理/资产授权列表]，点击<创建授权规则>按钮，进行规则的新建。

节点，对应的是资产，代表该节点下的所有资产。

用户组，对应的是用户，代表该用户组下所有的用户。

系统用户，及所选的用户组下的用户能通过该系统用户使用所选节点下的资

产。

动作，可设置上传、下载限制。

节点，用户组，系统用户是一对一的关系，所以当拥有 Linux、Windows 不同类型资产时，应该分别给 Linux 资产和 Windows 资产创建授权规则。

资产或节点可以授权给个人或用户组，一个授权建议只指定一个系统用户(多系统用户会按照优先级进行排序，高优先自动登陆，同时存在多个并级系统用户时，用户需要自己选择系统用户)

7.1.3. 更新授权规则

进入[权限管理/资产授权列表]，点击<更新>按钮，对已有的规则进行变更。

7.1.4. 删除授权规则

进入[权限管理/资产授权列表]，点击<删除>按钮，对已有的规则进行删除。

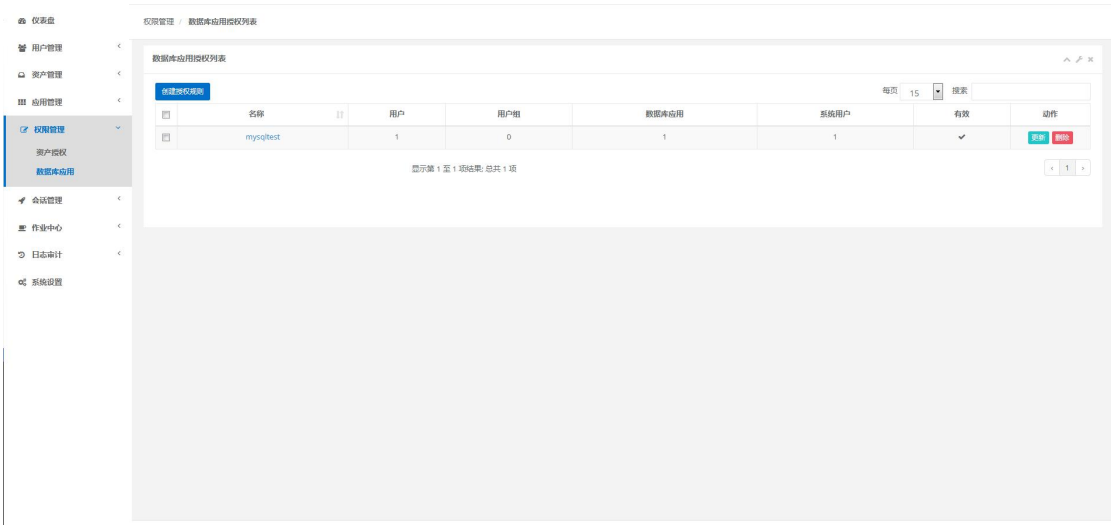
7.1.5. 查询授权规则

进入[权限管理/资产授权列表]，点击搜索栏，输入规则名称关键字，对规则进行筛选。

7.7. 数据库应用

数据库应用授权规则是针对数据库资产管理的授权规则。

7.2.1. 数据库应用规则列表



7.2.2. 创建数据库应用规则

进入[权限管理/数据库应用]页面，点击<创建授权规则>，如下图。

7.2.3. 更新数据库应用规则

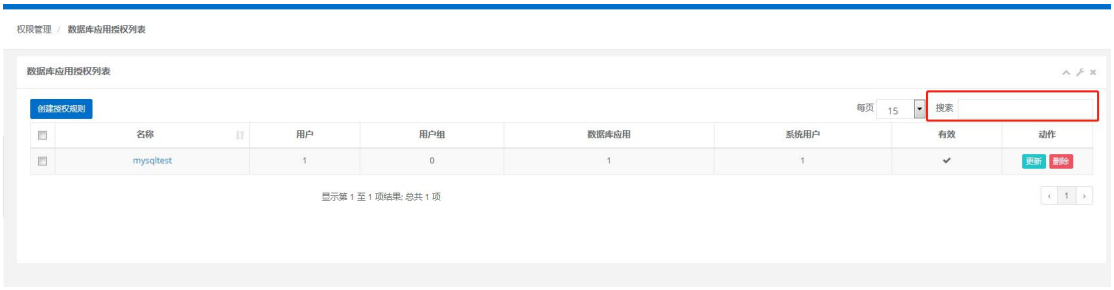
进入[权限管理/数据库应用授权列表]，点击<更新>按钮，对已有的规则进行变更。

7.2.4. 删除数据库应用规则

进入[权限管理/数据库应用授权列表]，点击<删除>按钮，对已有的规则进行删除。

7.2.5. 查询数据库应用规则

进入[权限管理/数据库应用规则列表]，点击搜索栏，输入规则名称关键字，对规则进行筛选。



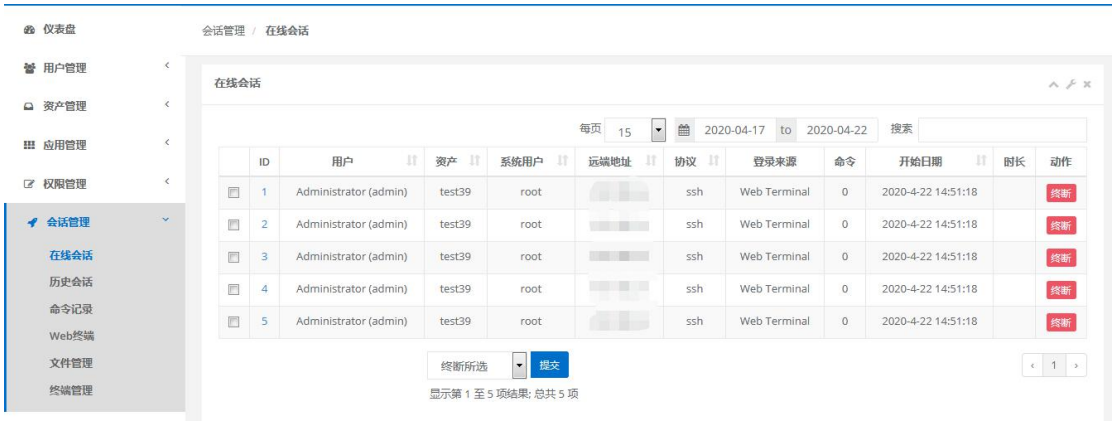
第九章. 会话管理

8.1. 在线会话

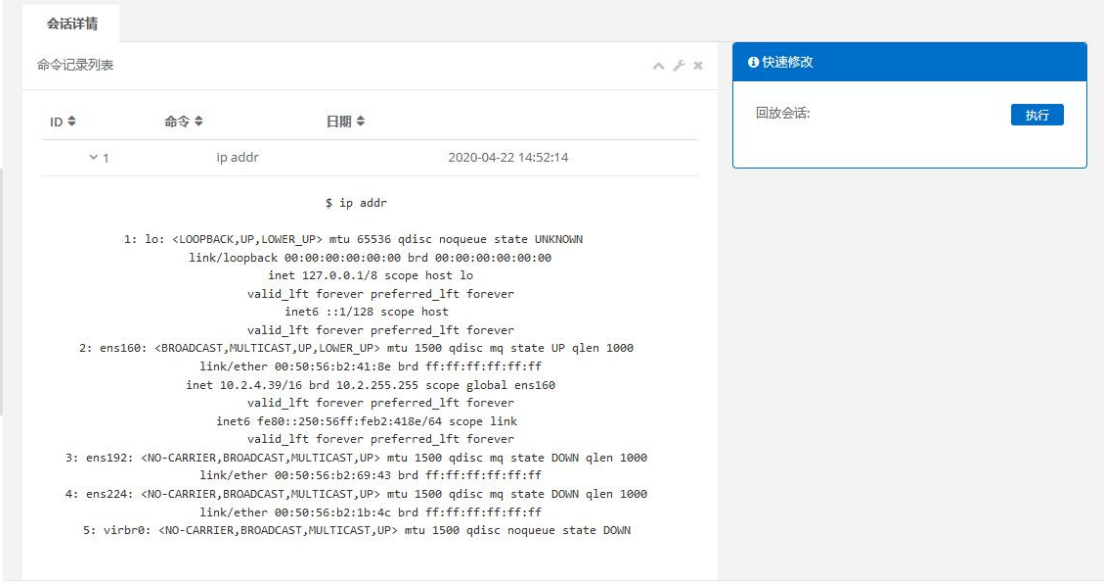
8.1.1. 查看在线会话

进入[会话管理/在线会话]页面，进入在线会话列表页面，默认展示最近 6 天的记录。用户：云翼运维审计系统在线的用户名。资产：登录的资产名称。系统用户：用户使用那哪个系统用户登录的资产。远端地址：登录用户的 IP 地址。命令：用户执行了多少条命令。开始日期：登录的时间。

点击搜索项，弹出搜索项下拉列表，可使用用户、资产、系统用户、远端地址、协议进行搜索。

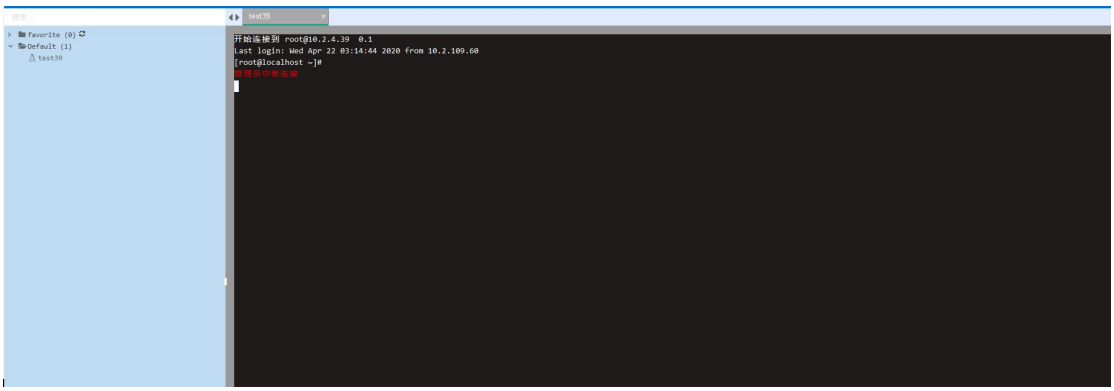


点击对应 ID 号，可进入该会话详情页面



8.1.2. 中断在线会话

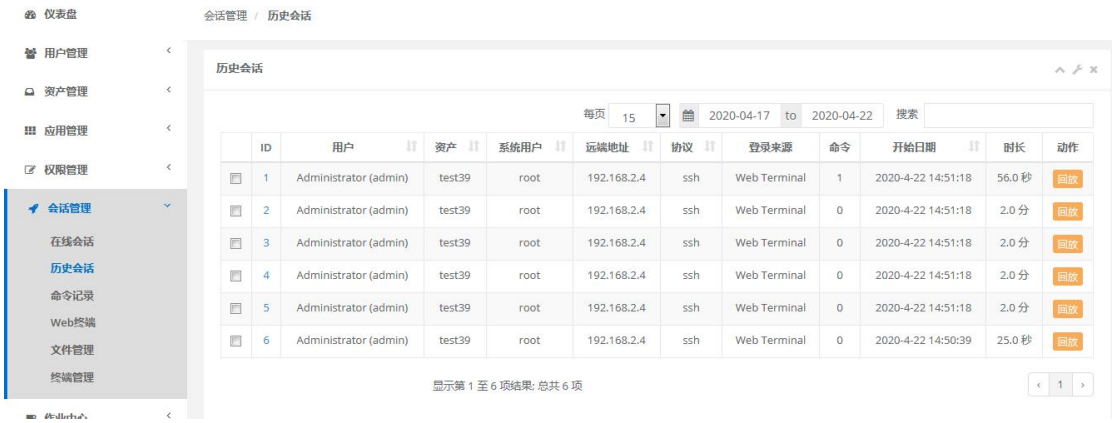
管理员可以手动中断当前在线的会话。已中断的会话会记录到"历史会话"里面。点击需要中断的对话最右侧的<中断>按钮，强制断开该会话。会话中断时，会话界面会有提示。管理员也可以选中多个会话，点击列表左下角的<中断所选>，并提交。



8.2. 历史会话

8.2.1. 历史会话列表

进入[会话管理/历史会话]，如下图所示。

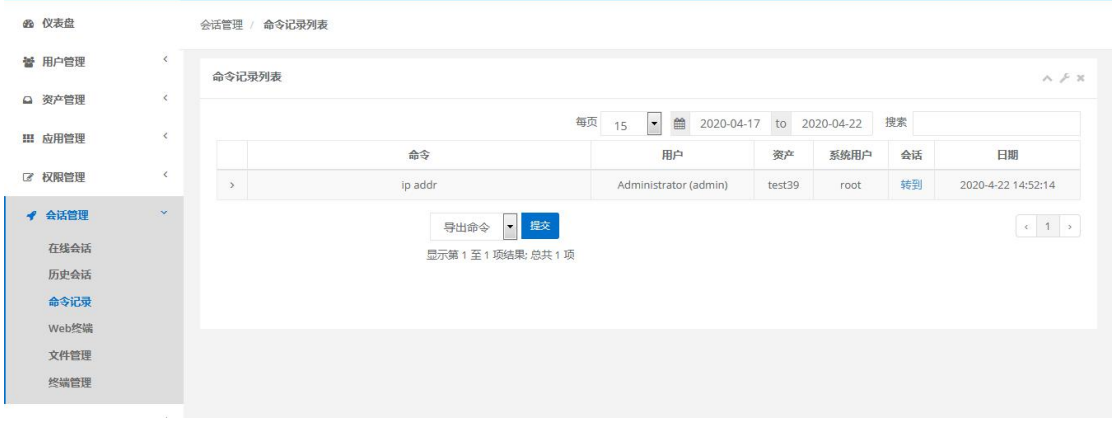


点击对应 ID 号会进入历史会话详情页面；点击<回放> 进入历史会话播放页面。

点击搜索项弹出搜索项下拉列表。可使用资产、用户、系统用户、远端地址、协议进行搜索。

8.3. 命令记录

命令记录里面存放的是用户在资产上执行过哪些命令，单击一行记录，会展示命令执行的结果：



点击"转到"连接，会跳转到详细的会话页面，如果会话已结束可以查看会话录像，如果会话正在线可中断会话。

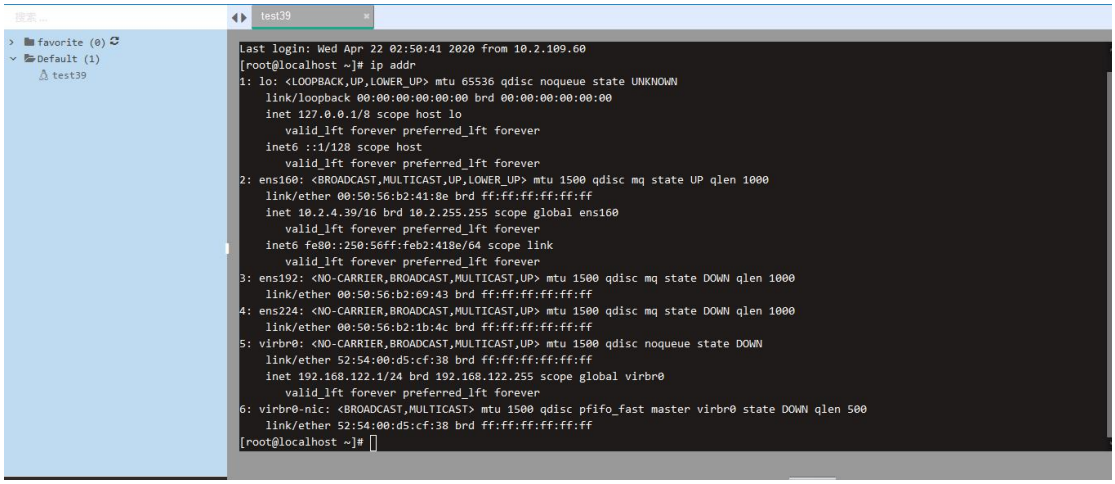
同样该列表也支持搜索，可使用用户、资产、系统用户、命令关键字进行搜索。

选择页面左下方的<导出命令>，点击提交。可将记录列表里面的命令导出到 html 文件。

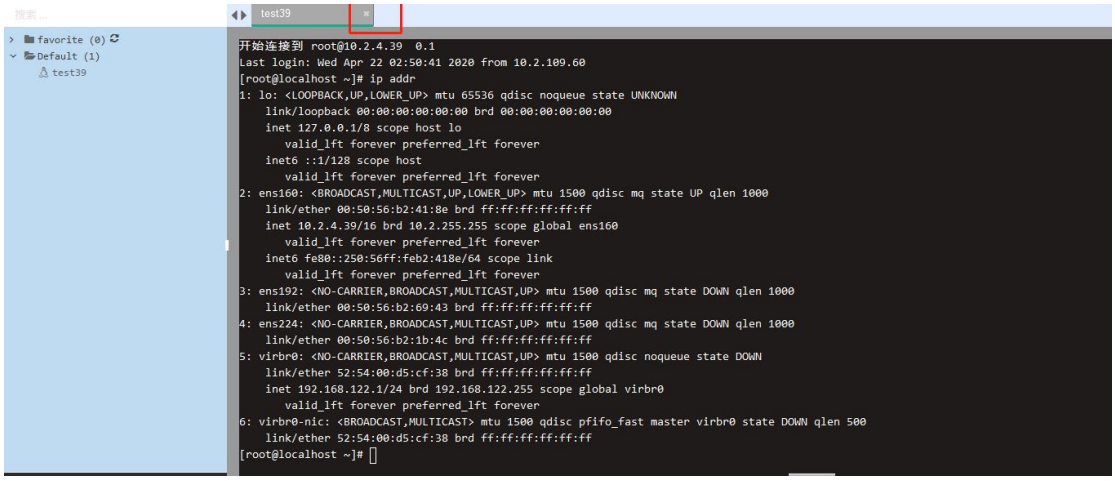
8.4. Web 终端

Web 终端是资产使用界面，管理员和用户都是从这里登录到资产上，执行操作。

点击资产名字连接资产。



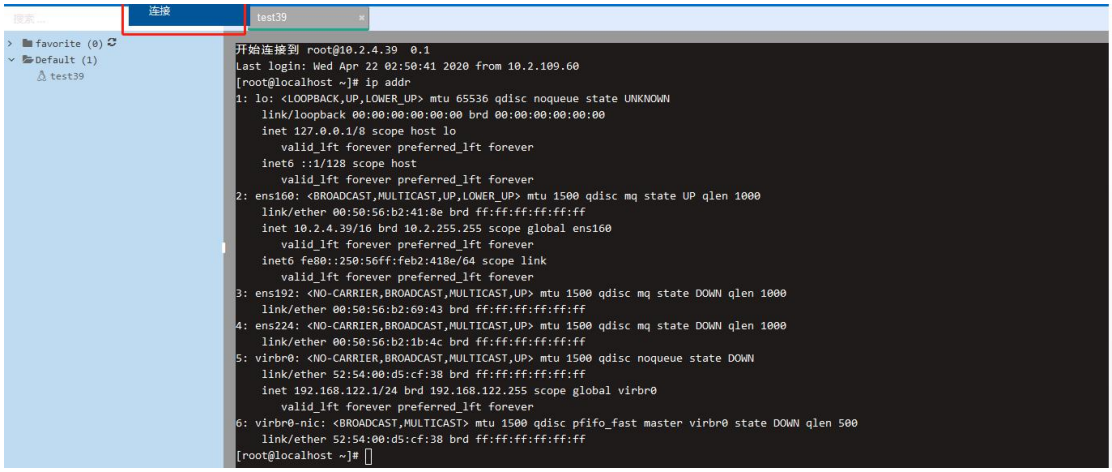
从系统断开连接或者点击标签页上的叉号都可以断开资产连接。



8.5. 文件管理

文件管理允许对 SSH 协议资产进行文件上传下载创建删除操作(不支持上传文件夹)，目前也不支持系统用户是手动登录的资产。

可以在[会话管理/Web 终端]下选择要进行文件管理的服务器后，从<文件管理/连接>进入，也可以从[会话管理/文件管理]，选择服务器进入。



进入文件管理后的界面如下：

8.5.1. 上传文件

使用菜单按钮进行文件操作时，请见下图功能注释。

还可以直接将文件拖拽至窗口空白处进行文件上传。

8.5.2. 文件管理

在选定的文件上点击右键，出现如下图所示菜单，选择对应的操作即可。

如果是文档类型的文件，在<下载>选项右侧会出现<链接>图标，点击图标可在线预览文档。

8.6. 终端管理

终端列表页面列出了云翼运维审计系统正在使用的终端有哪些，例如：koko、Gua 等。终端第一次使用，会首先向云翼运维审计系统发送请求注册，在云翼运维审计系统中接受注册后就可以正常使用该终端了。

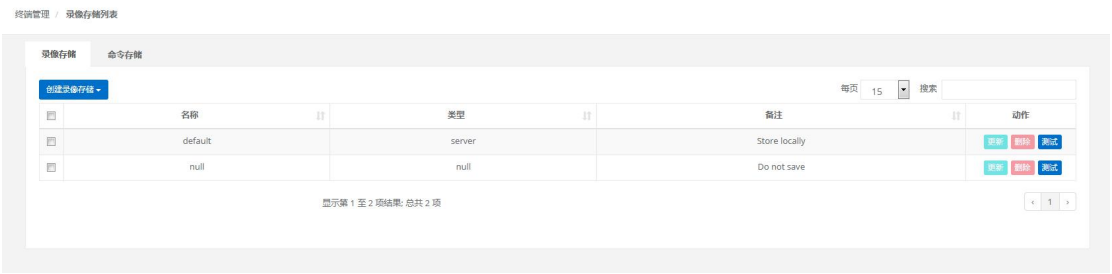
Koko 为 SSH Server 和 Web Terminal Server 。用户可以使用自己的账户通过 SSH 或者 Web Terminal 访问 SSH 协议和 Telnet 协议资产。

Gua 为 RDP 协议和 VNC 协议资产组件，用户可以通过 Web Terminal 来连接 RDP 协议和 VNC 协议资产 (暂时只能通过 Web Terminal 来访问)

如果这两个组件提供的功能出现问题，可以在这里进行删除重建。

8.6.1. 存储配置

在[终端管理/存储配置]页面，可以为录像和命令记录设置存储路径。



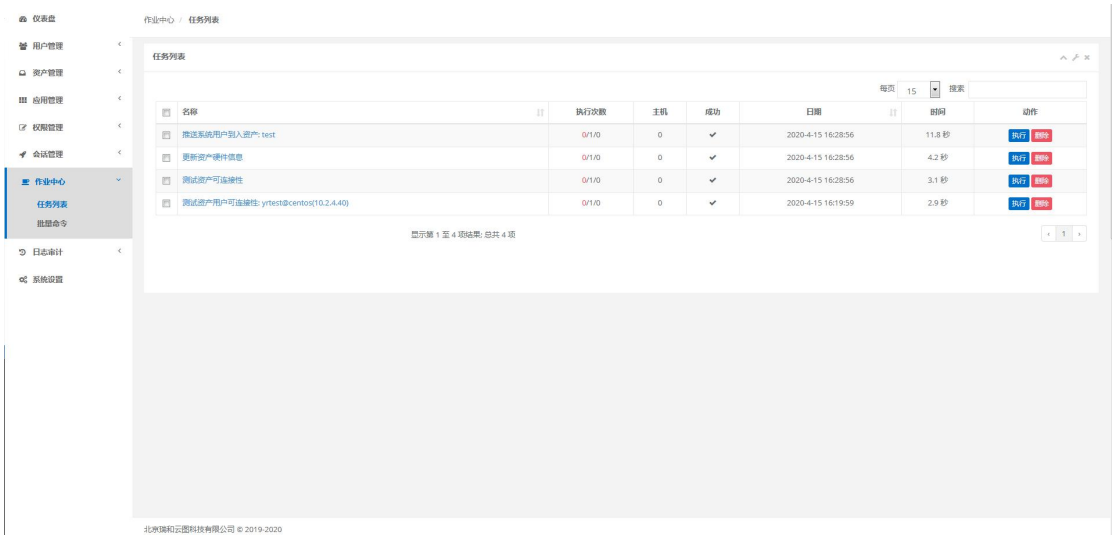
云翼运维审计系统支持的录像存储类型包括 S3、OSS、Azure、Ceph 以及 Swift，另外还包含默认存储类型 default（存储到本地）和 null（不存储）。

命令存储类型为 Elasticsearch，同时也包含默认存储类型 default（存储到本地）和 null（不存储）。

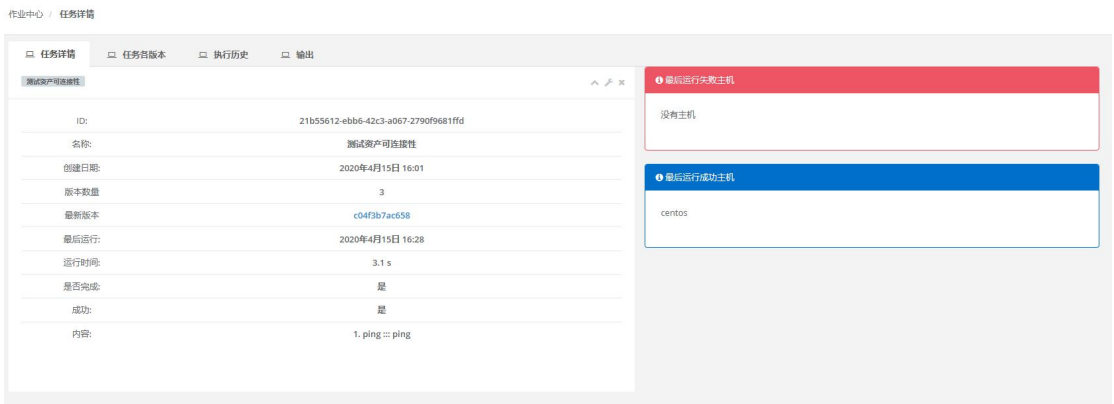
第十章. 作业中心

9.1. 任务列表

作业是云翼运维审计系统向其所管理下的资产发送的指令，例如测试资产可连接性、获取资产硬件信息、测试管理用户可连接性和测试系统用户可连接性等命令。默认展示最近 7 天的作业记录。其中，执行次数对应的数字分别为失败/成功/总计。

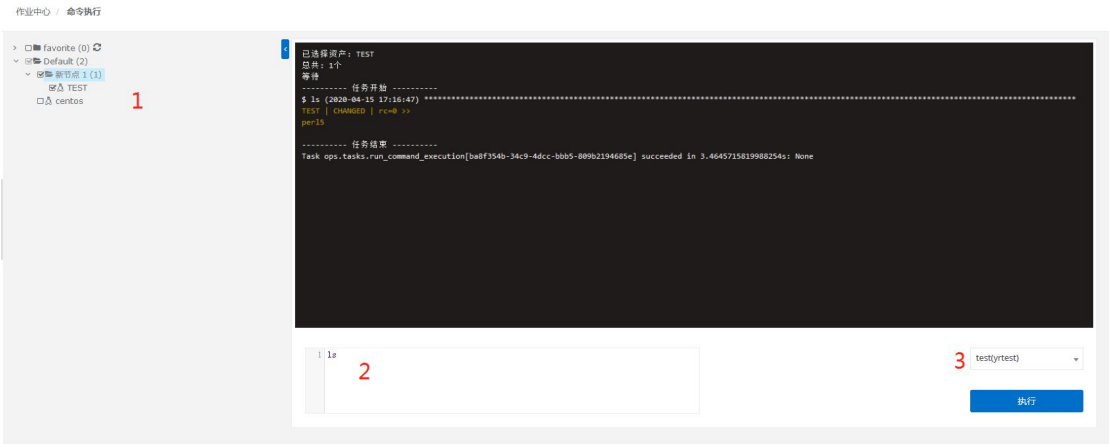


点击作业名称可以查看作业的具体详情、作业的历史版本以及作业执行的历史记录。



9.2. 批量命令

此功能可以快速下发命令到资产，目前仅支持能被 ansible 管理的资产，要求系统用户登陆方式为自动登陆。



1：要批量下发命令的资产；2：要执行的命令；3：选择用于执行命令的管理用户，该用户决定左侧资产树中所对应的资产；4：执行批量命令。

注意，如果想在 Windows 下执行批量命令，则需要把 Windows 的资产中增加一个 SSH 的协议组，如何配置请查看 5.1.2 创建资产。

9.3. 任务监控

云翼运维审计系统后台使用 Celery 作为分布式消息队列工具，用 Flower 作为它的监控和管理工具。任务监控界面就是 Flower 的管理界面。为管理员排错提供帮助。关于 Flower 和 Celery 的更详细说明请查看以下链接：

Celery：https://www.celerycn.io/ru-men/celery-jian-jie

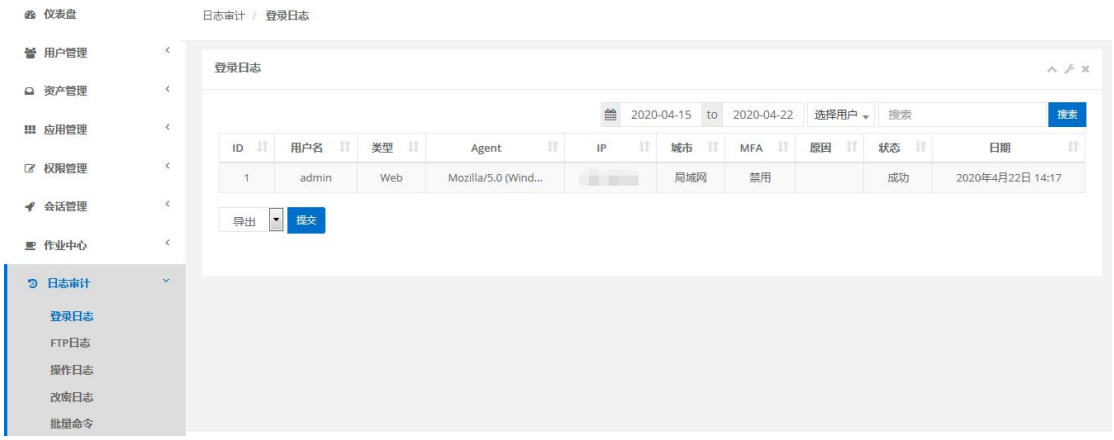
Flower：https://www.jianshu.com/p/4a408657ef76

第十一章. 日志审计

日志审计为用户提供了云翼运维审计系统登录日志以及操作日志等审计功能。

10.1. 登录日志

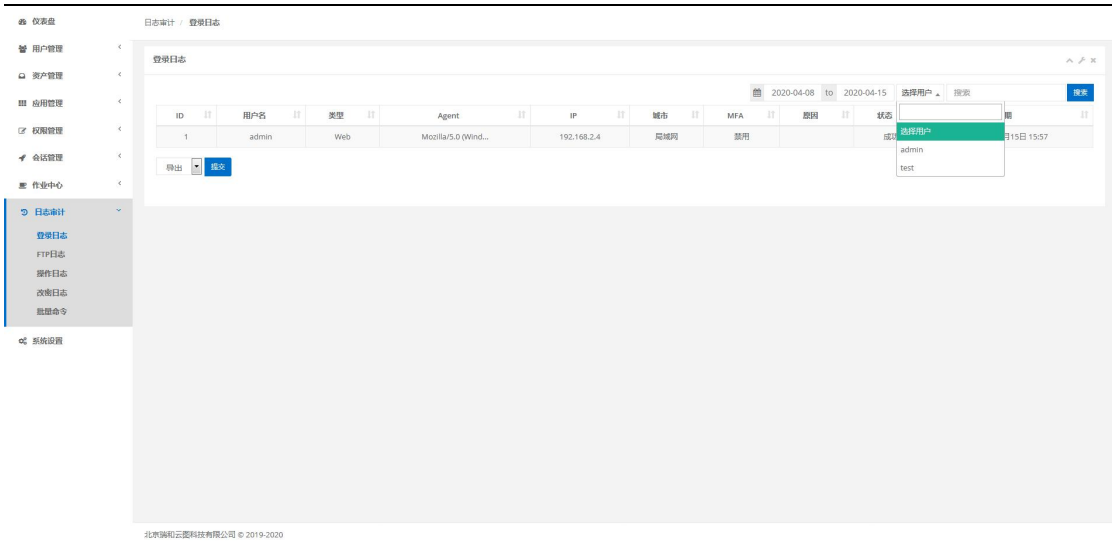
默认显示最近 7 天的云翼运维审计系统的登录日志。



10.1.1. 日志查询

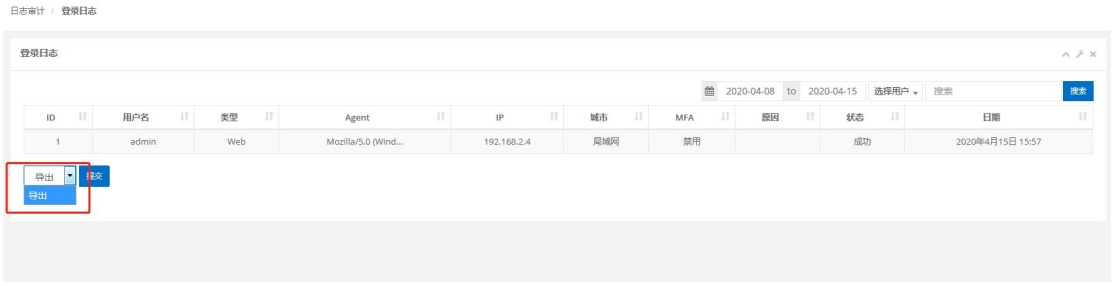
可用时间进行列表排序；可用用户名称进行筛选。

点击搜索项，可使用用户、来源 IP、城市进行搜索。



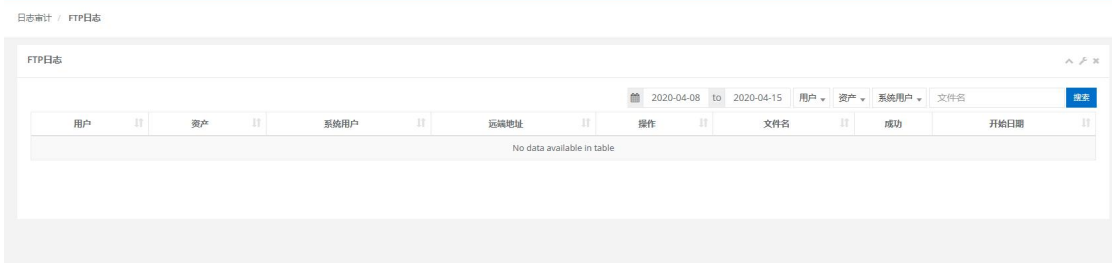
10.1.2. 日志导出

在页面左下角还可点击<导出>导出全部 CSV 格式的登录日志。



10.2. FTP 日志（无数据）

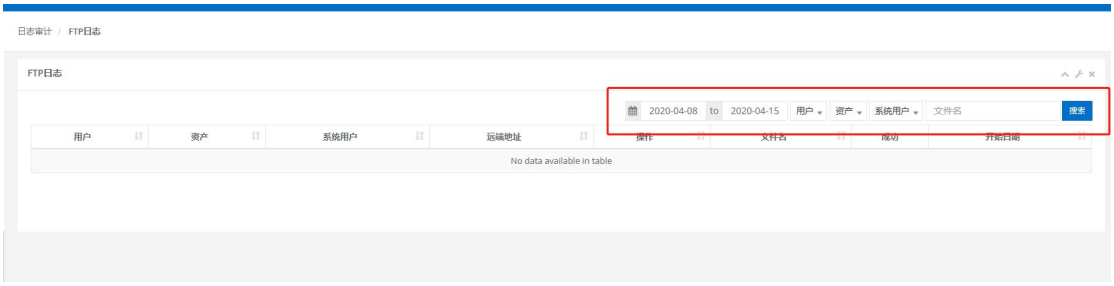
默认显示最近 7 天的云翼运维审计系统文件上传下载的日志。



10.2.1. FTP 日志查询

可进行列表排序；可用用户、资产、系统用户进行筛选。

点击搜索项，可使用文件名进行搜索。

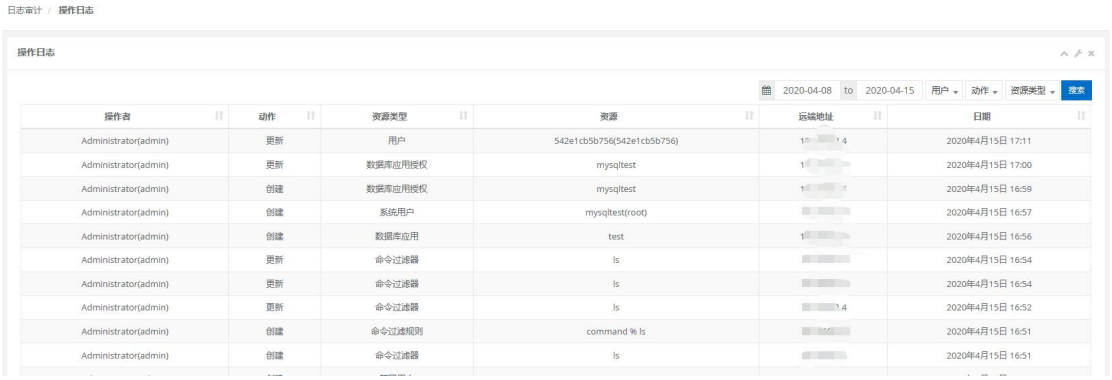


10.3. 操作日志

系统操作日志记录用户在云翼运维审计系统中的各种操作日志。

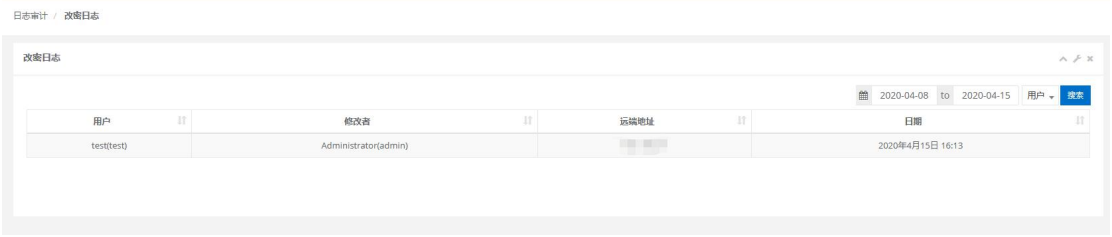
日志可进行列表排序；可对用户、动作、资源类型进行筛选。

资源类型包括：用户、用户组、资产、节点、管理用户、系统用户、网域、网关、组织、资产授权、命令过滤器、命令过滤规则。



10.4. 改密日志

默认显示最近 7 天云翼运维审计系统中用户修改密码的日志。



10.5. 批量命令

默认显示最近 7 天的批量命令执行情况。主机列对应的数字是该批量命令所执行的资产数。可根据用户名称进行筛选，右侧搜索框中输入命令关键字，可筛选相关命令的执行结果。

10.5.1. 批量命令执行详情

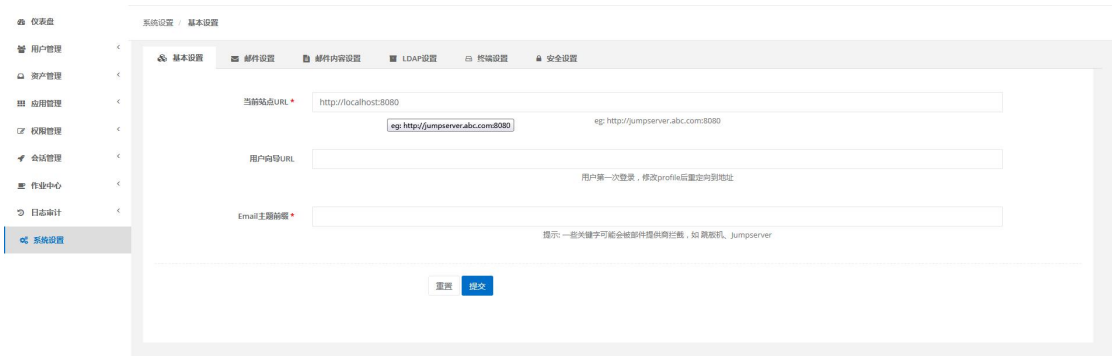
点击结果中的<详情>，页面自动跳转至批量命令执行结果页面。

第十二章. 系统设置

点击页面左侧“系统设置”按钮，进入系统设置页面，查看基本设置、邮件设置、LDAP 设置和终端设置等内容。

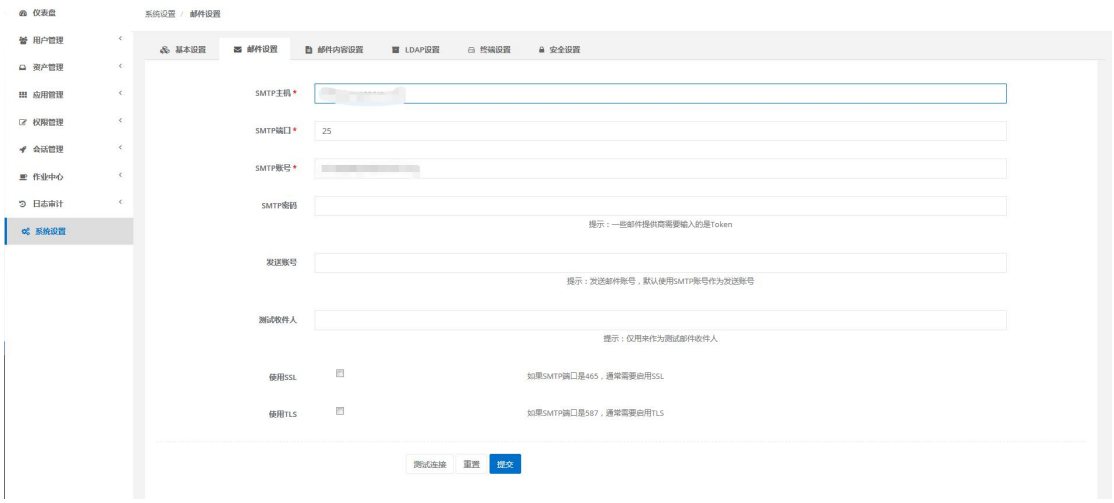
11.1. 基本设置

点击页面上边的“基本设置”按钮，进入基本设置页面，编辑当前站点 URL、用户向导 URL、Email 主题前缀等信息，点击“提交”按钮，基本设置完成。



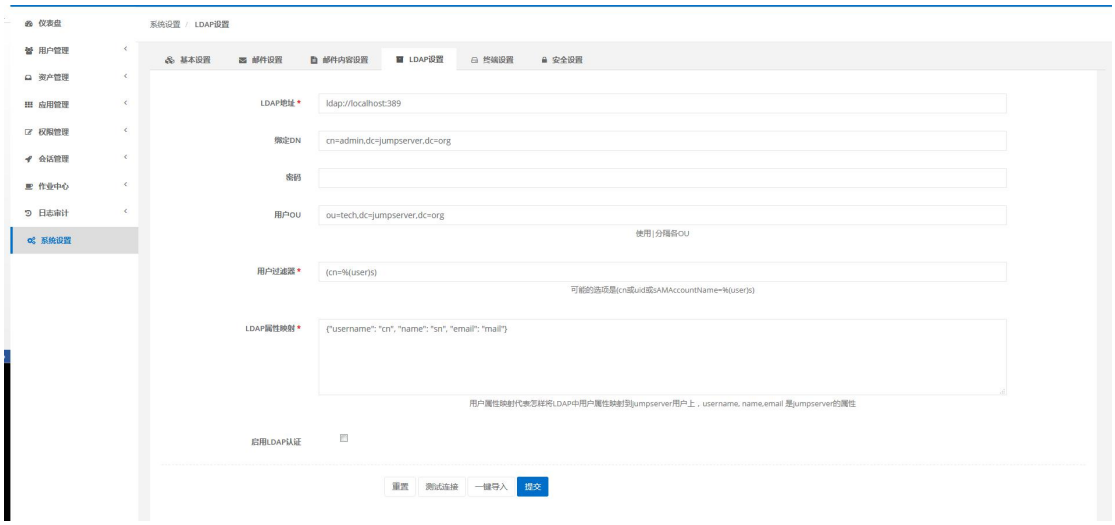
11.2. 邮件设置

点击页面上边的 "邮件设置" 按钮，进入邮件设置页面：



11.3. LDAP 设置

点击页面上边的“LDAP 设置”按钮，进入 LDAP 设置页面，编辑 LDAP 地址、DN、用户 OU、用户过滤器、LDAP 属性映射和是否使用 SSL、是否启用 LDAP 认证等信息，点击“测试连接”按钮，测试是否正确设置，点击“提交”按钮，完成 LDAP 设置。



11.4. 终端设置

点击页面上边的“终端设置”按钮，进入终端设置页面，编辑终端信息，点击“提交”按钮，终端设置完成。

资产列表排序项，可以选择按主机名或者 IP 来排序，默认是按主机名排序。心跳间隔指的是 koko 和 Gua 等终端向云翼运维审计系统发送心跳信息的频率，如果云翼运维审计系统长时间(1 个小时)未收到 koko 和 Gua 发送的心跳数据，云翼运维审计系统则认为该终端已经“宕机”，在“会话管理”下的“终端管理”页面会显示该终端已掉线。

11.5. 安全设置

点击页面上边的“安全设置”按钮，进入安全设置页面。

此页面包含安全设置和密码校验规则。

11.6. Syslog 日志设置

1、vi /etc/rsyslog.conf，找到

remote host is: name/ip:port, e.g. 192.168.0.1:514, port optional

#*.* @@remote-host:514

2、在后面添加*.* @logserverip:514

3、保存配置文件。