H3C-Seccloud 安全云管理平台

开局指导（融合 5.0 系列）

新华三技术有限公司
http://www.h3c.com

目 录

1 安全云背景介绍 1-2

1.1 产品介绍 1-2

1.2 组网 1-3

2 安全云管理平台安装指导 2-1

2.1 注意事项 2-1

2.2 安装包 2-1

2.3 H3C SecCloud OMP 安全云管理平台部署 2-1

2.3.1 安装安全云组件包 2-1

2.3.2 验证安全云部署结果 2-5

3 云操作系统初始化配置指导 3-6

3.1 创建组织和用户 3-6

3.2 配置安全资源池 3-7

3.2.1 VNF 方式 3-7

3.2.2 资源池方式 3-10

3.3 分配配额 3-27

3.4 设置资源规格 3-29

1 安全云背景介绍

在数字化转型的过程中，IT 架构也正在发生着巨大的变化，传统烟囱式的建设模式，每个业务系统拥有相互独立的安全防护设备，这种碎片化的安全架构已完全不能够适应业务架构的融合与扩张，也会由于带宽加大和应用的多样性成为安全系统部署的最大瓶颈。为解决上述问题，新华三提出了安全云的解决方案，重新定义在新 IT 架构下的安全能力。安全云从用户业务的角度出发，将安全能力的配置抽象为必要的逻辑实现。使安全能力具备快速部署、租户级细粒度安全防护、安全可视化管理等特点。

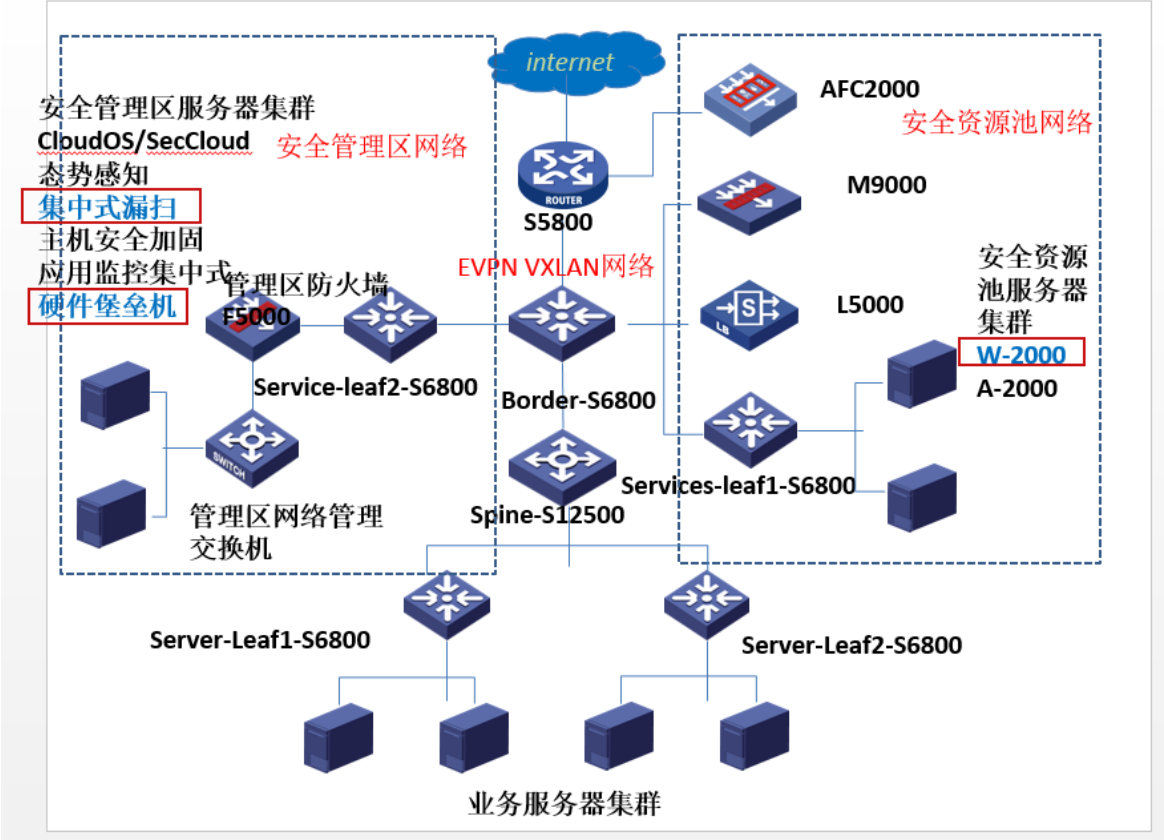
1.1 产品介绍

安全云系统是一款全新设计的适用于云计算网络的云安全服务管理平台。安全云从逻辑控制层的角度出发，屏蔽底层技术细节，将繁琐的安全业务重新进行定义，从用户业务的角度出发，为用户提供抽象的各类安全能力的服务化配置和管理。

安全云本质是一个安全设备的管理平台，通过该平台，将用户的安全设备纳管，仅仅通过安全云即可实现对一系列安全设备下发配置、修改配置、查看状态等功能，即通过安全云可以实现安全设备的快速部署、安全能力的差异化部署、及安全状态的可视化功能。安全云资源池网络提供服务器安全监测、漏洞扫描、数据库审计、安全专家服务、堡垒机、DDoS 服务、Web 应用防护、日志审计、应用监控、态势感知、第三方安全 11 种安全服务业务。

1.2 组网

图1-1 组网图



安全云管理平台作为一个管理平台，作用于 EVPN Vxlan 整体组网方案中。该典型组网逻辑上大体分为三部分，逻辑上的左侧部分为安全云管理区，管理区部署了安全云管理平台、CloudOS、VCFC、态势感知、集中式漏扫、集中式应用监控服务、主机安全防护服务的管理端等以提供给租户管理自身安全服务设备。其中安全云管理平台是 CloudOS 的一个组件，部署于 CloudOS 之上；VCFC 是实现了 EVPN Vxlan 网络；服务器安全监测、漏洞扫描、数据库审计、安全专家服务、堡垒机、DDoS 服务、Web 应用防护、日志审计、应用监控是安全云所纳管的部分安全服务。逻辑上的右侧部分为安全资源池区，包含 DDOS 设备、防火墙设备、负载均衡设备、安全资源池 CAS 集群，其中安全资源池 CAS 集群的作用是提供日志审计、数据库审计、运维审计、Web 应用防护四种服务的虚拟机环境。逻辑上的下侧部分为用户的业务服务器集群，该部分是安全云管理平台所纳管的安全设备进行防护的区域。

表1-1 开局设备及版本

设备	版本	备注
安全云管理平台OMP	H3C-SecCloud-E1108	
安全资源池区CAS集群	H3C_CAS-E0513	
Cloudos 云操作系统	E5102	
漏洞扫描	H3C SecPath SysScan 3.10- E6903P01	

堡垒机	SecPath2000AV-IMW310- E6112P03	
数据库审计	H3C SecPath SysScan 3.10- E6204P06	
DDoS防护	串联防护：H3C i-Ware Software, Version 1.10, ESS 6503 旁路防护：H3C i-Ware Software, Version 1.10, ESS 6503P01 检测设备：H3C i-Ware Software, Version 1.10, ESS 6503P01	
Web应用防护	H3C i-Ware Software, Version 3.1, ESS 6203	
服务器安全监测	E6402L02	
应用监控	H3C i-Ware Software, Version 3.10, ESS 6801	需安装补丁，由研发提供
日志审计	CSAP-SA-V E1104	

2 安全云管理平台安装指导

2.1 注意事项

部署工作开始前请参考本章内容完成相应的准备工作，以免部署过程中遇到无法预知或控制的问题。其准备工作如下：

- H3C CloudOS 云操作系统正确部署且运行正常，其中云操作系统的版本必须为 E5102；
- H3C SecCloud OMP 安全云管理平台与 CloudOS 云操作系统的 E5102 版本适配。

2.2 安装包

H3C SecCloud OMP 安全云管理平台对外提供的组件包如下：

- 系统组件包：H3C-SecCloud-EXXXX.zip，其中的 XXXX 表示具体的版本号。在部署前，建议参考版本发布文档校验压缩包的 MD5 值是否一致。

2.3 H3C SecCloud OMP安全云管理平台部署

2.3.1 安装安全云组件包

(1) Cloudos 相关环境确认。

确保 CloudOS5102 正常工作，网络规划、计算可用域等配置正确。

图2-1 可用域

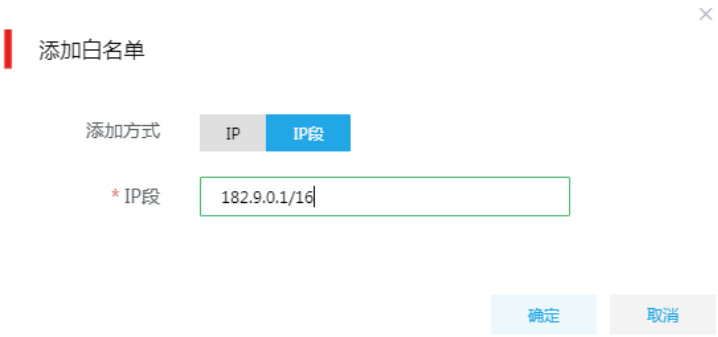
图2-2 计算节点

图2-3 网络规划

(2)　在 Cloudos 平台中增加 secaas 命名空间。

a.系统-系统配置-安全设置-数据库白名单，添加本地访问的 IP 段，可以允许本地数据库工具连接数据库。

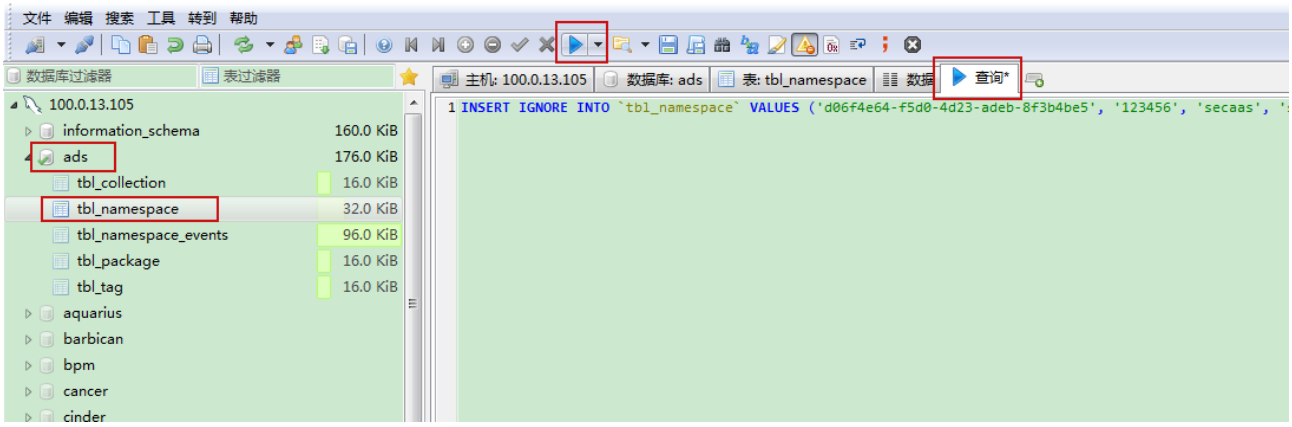
图2-4 添加数据库白名单可以是 IP 或者 IP 段



b.打开数据库，找到库 ads 和 tbl_namespace 表，执行如下 sql 脚本。

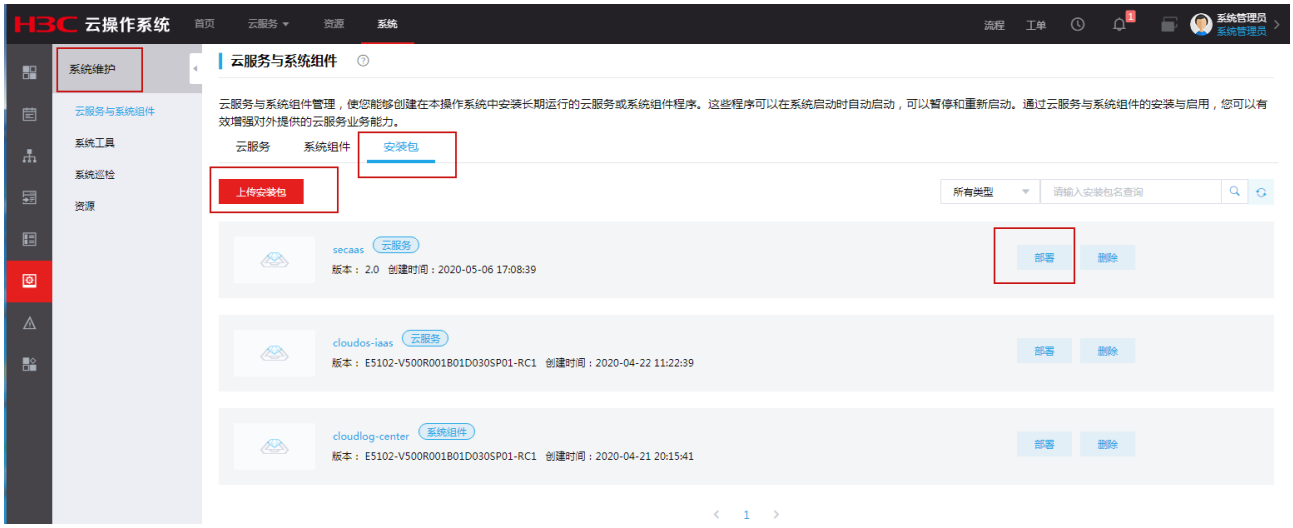
添加secaas命名空间.sql

图2-5 执行加域脚本



(3) 系统-系统维护-云服务-安装包，上传安装包（保存在本地的 zip 包）并部署。

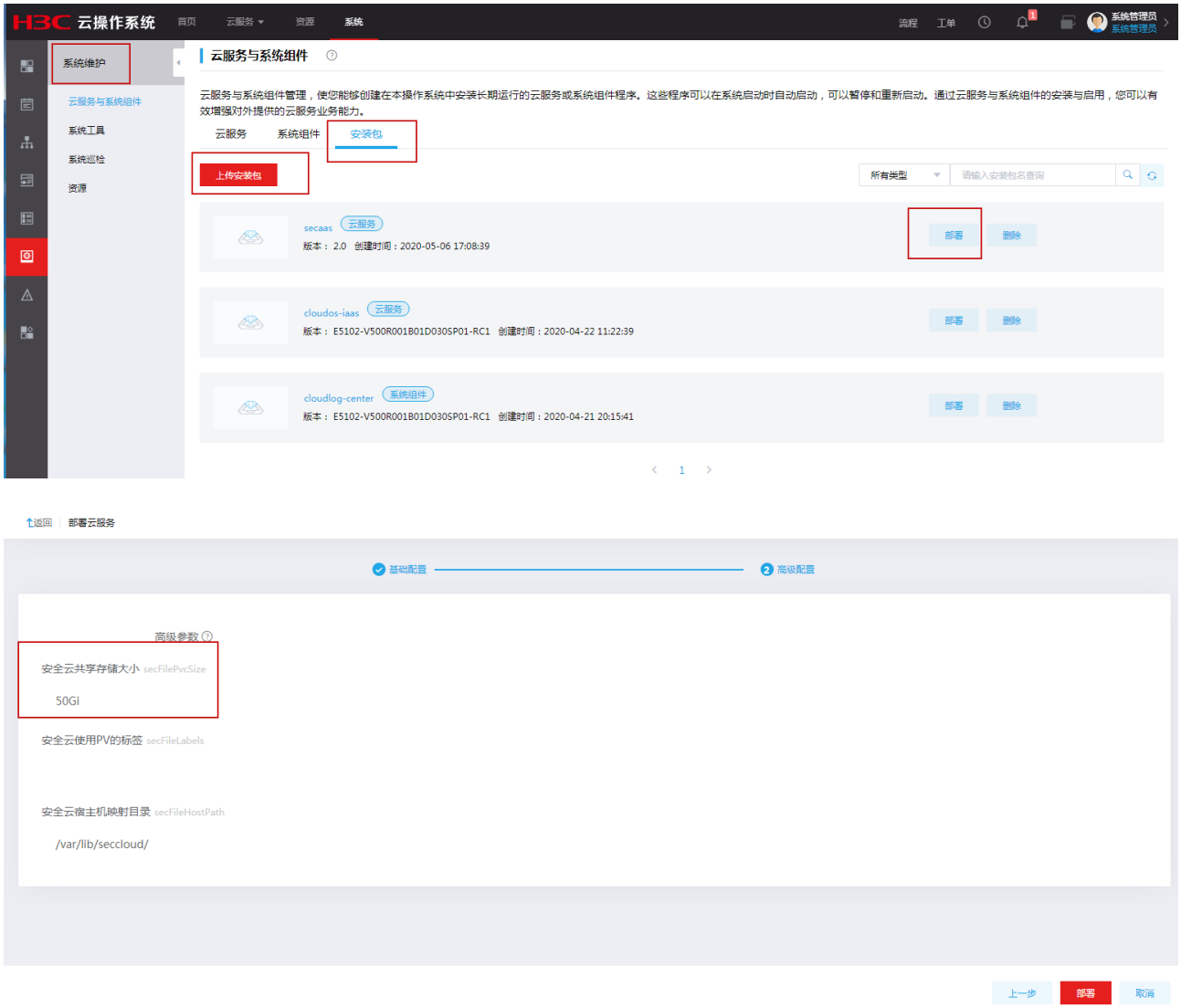
图2-6 上传安装包并部署



(4) 部署安全云组件需要一块共享存储，该共享存储建议不低于 50G。共享存储的准备方式根据现场所使用的共享存储工具来操作。推荐使用 ISCSI 共享存储，在服务器后台映射存储卷的方法，可参考《H3C CloudOS 5.0 云操作系统部署指导》中的 7.2 节。在 Cloudos 平台添加共享存储可参考《H3C CloudOS 5.0 云操作系统部署指导》中的 6.2 节。

(5) 系统-系统维护-云服务-安装包，上传 H3C-SecCloud-EXXXX.zip 并部署。

先上传安装包文件，再进行部署；



说明

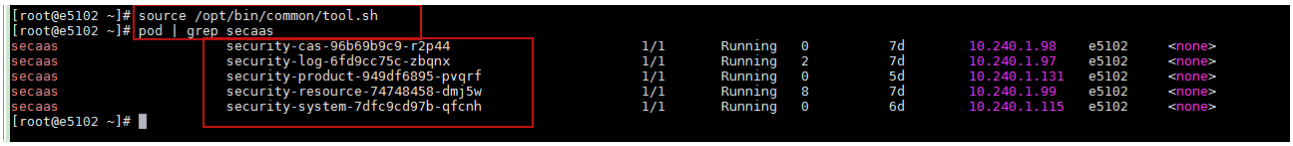
安全云使用 PV 的标签不需要填写，仅填写共享存储大小，推荐使用默认的 50G，映射目录使用默认值，不修改。

2.3.2 验证安全云部署结果

登录 CloudOS Master 节点的后台执行以下命令，查看与安全云相关的 pod 都是否处于 Running 状态。

```
source /opt/bin/common/tool.sh
pod | grep secaas
```

图2-7 检查是否有如下图红框中的内容



3 云操作系统初始化配置指导

云操作系统初始化相关的操作通过云管理员账户来进行，以 admin 用户登录云操作系统，进行初始配置：（1）创建组织和用户；（2）配置安全资源池；（3）分配配额；（4）设置资源规格。

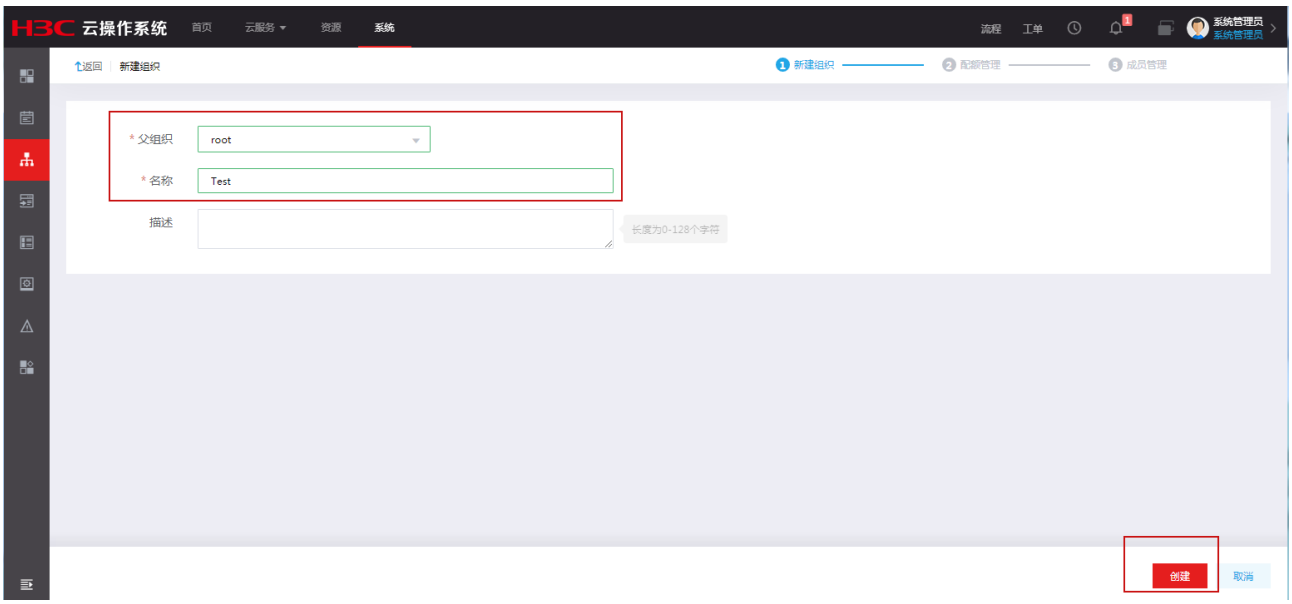
3.1 创建组织和用户

安全云目前有三种角色，三种角色分别为：系统管理员（云管理员）、组织管理员、普通用户。云管理员可进行组织、用户的创建，创建后，使用用户名、密码可访问云操作系统。

(1) 系统管理员创建组织

以云平台地址 100.0.13.105 为例，浏览器 URL 访问 http://100.0.13.105，使用系统管理员用户名/密码：admin/cloudos（具体以实际情况为准）登录云操作系统平台。单击[系统/组织管理]菜单项，单击新建组织，填写组织名称，选择父组织。

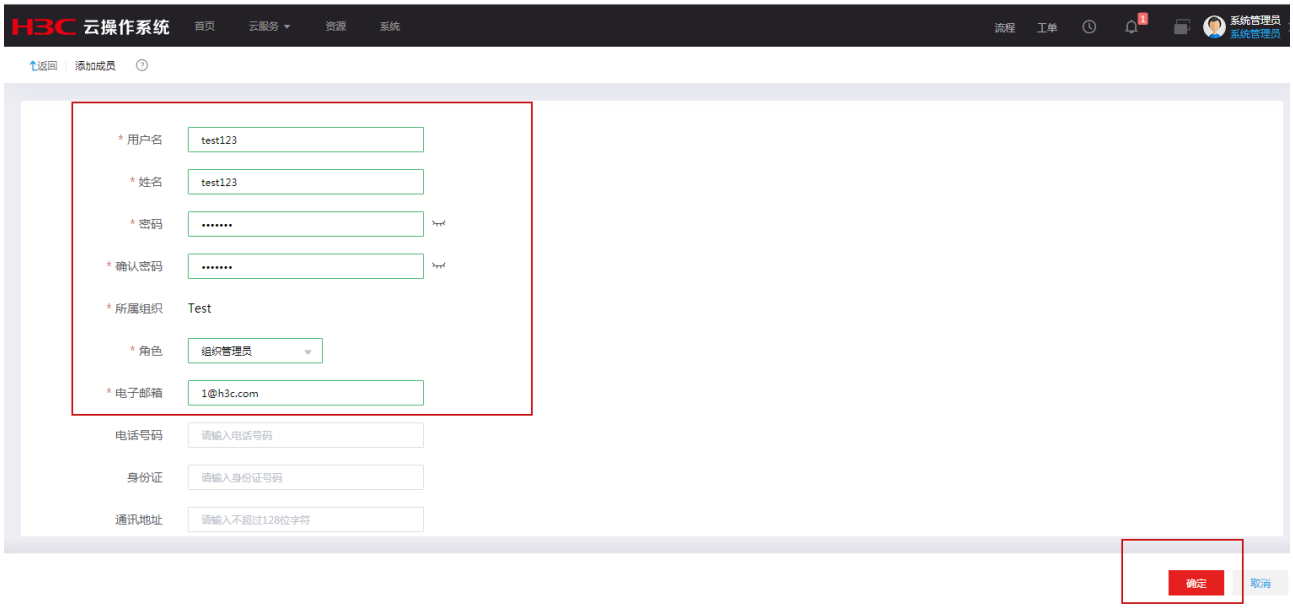
图3-1 创建组织



(2) 系统管理员创建用户

以云平台地址 100.0.13.105 为例，浏览器 URL 访问 http://100.0.13.105，使用系统管理员用户名/密码：admin/cloudos（具体以实际情况为准）登录云操作系统。单击[系统/组织管理]菜单项，选定组织，单击添加成员，填写必填的参数，其中用户分为组织管理员和普通用户，在角色字段可以进行选择。

图3-2 创建用户



3.2 配置安全资源池

安全云可通过两种方式为云内租户提供安全服务：（1）租户创建安全服务时，通过安全云自动创建虚机，下发管理地址网络，业务地址网络，并自动授权 License，方式一涉及到的安全服务有：堡垒机、数据库审计、WAF、日志审计，该方式简称 VNF；（2）系统管理员提前准备好安全资源，并添加至安全资源池内，租户创建服务，使用安全资源池内的安全资源，安全资源支持多租户共享或独享，方式二涉及到的安全服务有：服务器安全监测、漏洞扫描、DDOS、应用监控、堡垒机、数据库审计、WAF、日志审计，态势感知，该方式简称资源池。

使用 VNF 或资源池方式提供安全服务所需要进行的初始化配置方式不一样，下文描述不同方式需要进行的初始配置。

3.2.1 VNF 方式

1. 配置 CAS 资源池

以云平台地址 100.0.13.105 为例，浏览器 URL 访问 http://100.0.13.105，使用系统管理员用户名/密码：admin/cloudos（具体以实际情况为准）登录云操作系统。单击[资源/安全资源池/CAS 资源池]菜单项，进行 CAS 参数相关配置，具体参数解释如下：

- 用户名、密码、IP 地址：分别为登录云计算管理平台的用户名、密码、IP 地址；
- 主机池/集群：当用户名、密码、IP 地址配置好后，点击下一步，在主机池/集群中可下拉选择，选择需要安全虚机落在 CAS 中集群的位置；
- 存储池名称：默认为 defaultpool，若 CAS 中重新添加了存储池或修改了默认存储池的名称，则对该字段进行修改，与 CAS 中保持一致。

图3-3 存储池

- 虚机模板：下拉选择相应安全服务的虚机模板，注意不同规格对应特定的虚机模板；不同安全服务虚机模板需提前导入到 CAS 中，并配置 LicenseServer，具体导入和配置方式见《安全云虚拟化服务环境准备指导》文档。
- CAS 虚机网络参数配置：该部分为虚拟机管理网卡地址池相关参数配置，其中起始地址、结束地址、子网掩码、网关、DNS 字段可根据现场的实际网络情况进行配置。其中 VLAN-Vxlan 映射关系，需要与 VCFC 中[承载网络/VLAN-VXIAN 映射]VLAN 映射区间、VXIAN 映射区间保持一致。

图3-4 Vlan-VXLAN 映射表

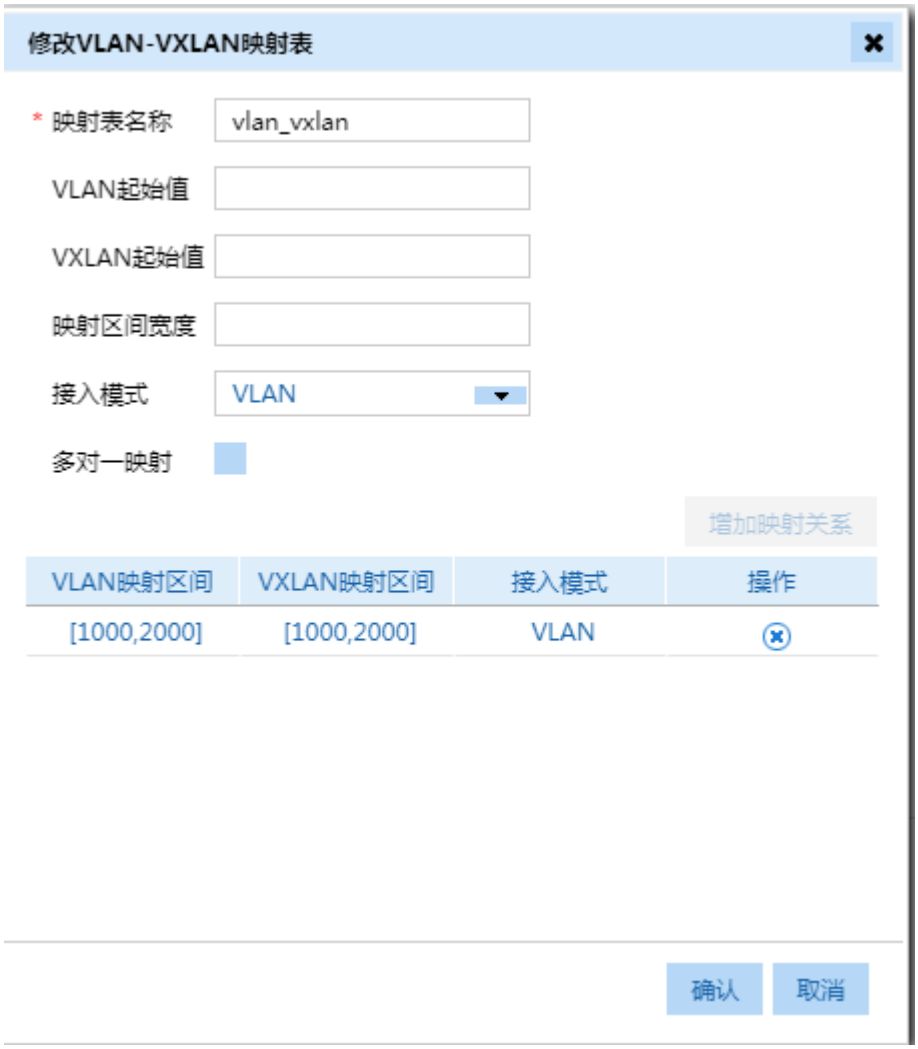
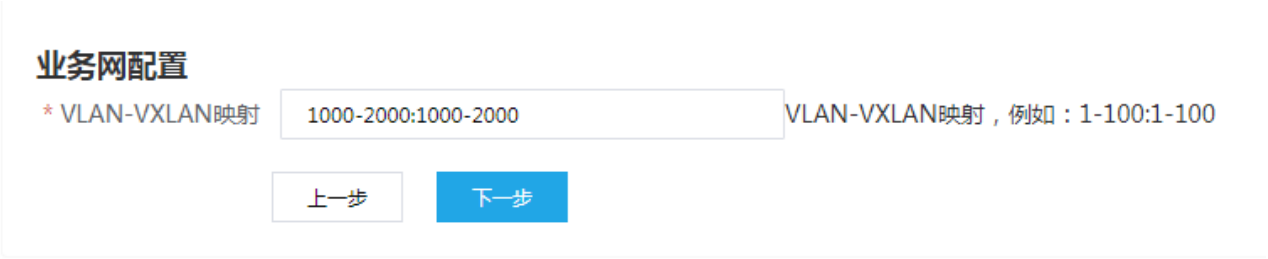


图3-5 CAS 资源池 VLAN-VXLAN 映射



2. 配置 LicenseServer 信息

WAF、堡垒机、数据库审计服务若以 VNF 形式提供服务，需要配置 LicenseServer 信息。以云平台地址 100.0.13.105 为例，浏览器 URL 访问 http://100.0.13.105，使用系统管理员用户名/密码：admin/cloudos（具体以实际情况为准）登录云操作系统。单击[资源/安全资源池]菜单项，对应 WAF、堡垒机、数据库审计资源池操作栏中，配置相应的 LicenseServer 信息。

图3-6 配置 LicenseServer 信息

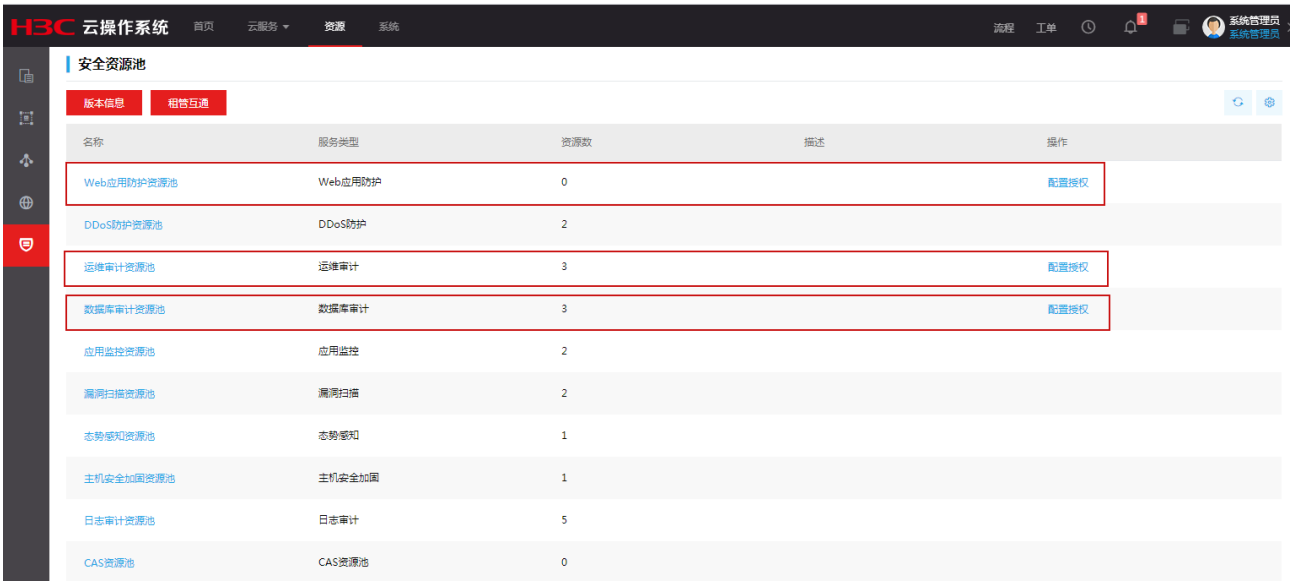


图3-7 WAF LicenseServer 信息配置

3.2.2 资源池方式

资源池方式需要系统管理员将安全资源添加至安全云资源池内，不同安全资源添加之前需要进行初始配置，不同的安全资源添加方式及注意事项不同，下文针对服务器安全监测、漏洞扫描、DDOS、应用监控、堡垒机、数据库审计、WAF、日志审计、态势感知 9 种安全服务描述不同的添加方式。

1. 日志审计资源池

(1) 日志审计资源准备

部署日志审计服务，形式可以为硬件日志审计服务或虚机日志审计服务，具体版本要求请参见[错误!未找到引用源。](#)。

开启硬件日志审计单点登录，进入后台

cd 到该目录下：

将单点登录的 false 改为 true

```
es.clusterNodes=lcahost\:9300
shiro.sso.enable=true
jdbc.driver=com.mysql.jdbc.Driver
spark.driver.memory=2048m
logImport.webIP=lcahost
ckla.name=ckla
shiro.localLogoutUrl=/toLogin
spark.monitor.baseUrl=http\://lcahost\:6790/v1/server/
redis.host=lcahost
shiro.cas.service=https\://100.0.20.7\:443/shiro-cas
logImport.db=15
log.addr=http\://lcahost\:8088/lca/v1
probe.addr=http\://lcahost\:28443/
spark.sparkMaster.create=http\://lcahost\:6066/v1/submissions/create
mas.task.exec.interval=60
jdbc.password=iQnQEHL6wjp9DkihY1b2SM7BTBmrIUN/kC2ovqAOruRAR2meArMiXcJ3fMlUnTB0JyHC4yGUwVVM1UyUyYG6owgYBaiSD/yeGazOZB+20fFFMv5K0w
x6h8jvVwgHhTrnTsJk/HgtchUYD4qL/SpRm+8srhaUiA9Y3nl1sjasD5yZ705gLmHmWkFHsLnXfUs6fXRM1aquXBebAY1zkTigJW1rWUjgtKBBizQjnlp9g5qyvngcDn
t4NEUQr0MxUro/MRfuTz2hacD/rfyQGEmdrnFtQcDPlB1FB5mpHZ4Vlcjp56DLzphe6BWzVlGyjfhm0eQ7ztmz5Od/MIOCw1MkpQ\=\=
redis.password=SH6TNKhmNMwHzEK/gp1fDW1j/TXrXusy32VgoIZ2Klq+2gOVfBYcJDgEKI9mXyEMJcgc/m5FMrOyAiGyoyenqMxJ4Jg8xm1trDnbsphNKKTfcfM/H
+IKDABRHZAO0BzeECn38zI9cR7knHQCyDfzRtwK9M/aFYfMIGd8sqLyTxIE3k+VitiLmk1MZrffag3ghEhu1e8K6dpzV6QCh58+01RkcHWoy3grAQndnZMsJ7GxHMF4s
D2kpsYigfs6EAP1FpAn3mre0mdtrMU3MoPSJTr4vy98aUvmWJNW4mih7pRMjCZAI12wQHwu4aqMyw4UrY5REH4NUdL7AFgRg/hW8Q\=\=
mas.task.scan.interval=600
jdbc.username=root
spark.mainClass=com.h3c.soc.das.eventcorrelation.sparkstreaming.KafkaRealtimeEventCorrelation
spark.num.executors=2
es.api.url=http\://lcahost\:8980/
shiro.logoutUrl=http\://100.0.13.106\:30001/cas/logout?service\=https\://100.0.20.7\:443/shiro-cas
saveDayN=30
```

重启 tomcat 有如下两种方式，

方式一：重启 tomcat 中日志审计服务

cd 到该目录下，执行./shutdown.sh

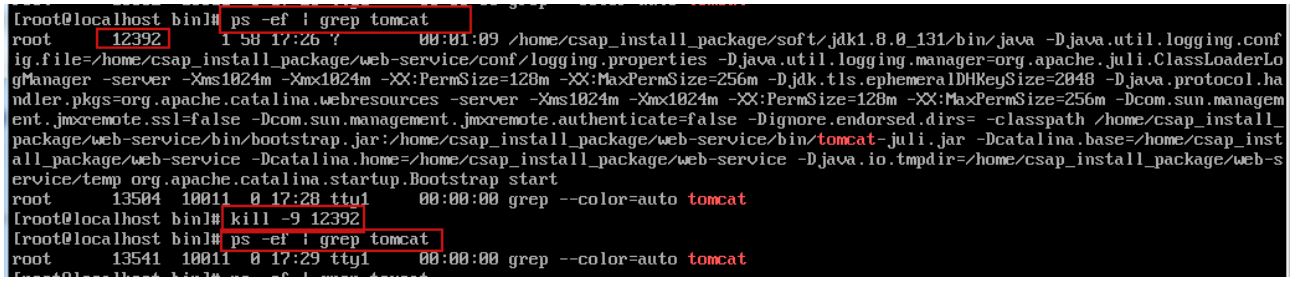
./startup.sh

```
[root@localhost bin]# pwd
/home/csap_install_package/web-service/bin
[root@localhost bin]#
[root@localhost bin]#
[root@localhost bin]#
[root@localhost bin]#
[root@localhost bin]#
[root@localhost bin]# ./shutdown.sh
Using CATALINA_BASE:   /home/csap_install_package/web-service
Using CATALINA_HOME:   /home/csap_install_package/web-service
Using CATALINA_TMPDIR: /home/csap_install_package/web-service/temp
Using JRE_HOME:        /home/csap_install_package/soft/jdk1.8.0_131
Using CLASSPATH:       /home/csap_install_package/web-service/bin/bootstrap.jar:/home/csap_install_package/web-service/bin/tomca
t-juli.jar
Java HotSpot(TM) 64-Bit Server VM warning: ignoring option PermSize=128m; support was removed in 8.0
Java HotSpot(TM) 64-Bit Server VM warning: ignoring option MaxPermSize=256m; support was removed in 8.0
[root@localhost bin]# ./startup.sh
Using CATALINA_BASE:   /home/csap_install_package/web-service
Using CATALINA_HOME:   /home/csap_install_package/web-service
Using CATALINA_TMPDIR: /home/csap_install_package/web-service/temp
Using JRE_HOME:        /home/csap_install_package/soft/jdk1.8.0_131
Using CLASSPATH:       /home/csap_install_package/web-service/bin/bootstrap.jar:/home/csap_install_package/web-service/bin/tomca
t-juli.jar
Tomcat started.
[root@localhost bin]# _
```

方式二：重启整个 tomcat

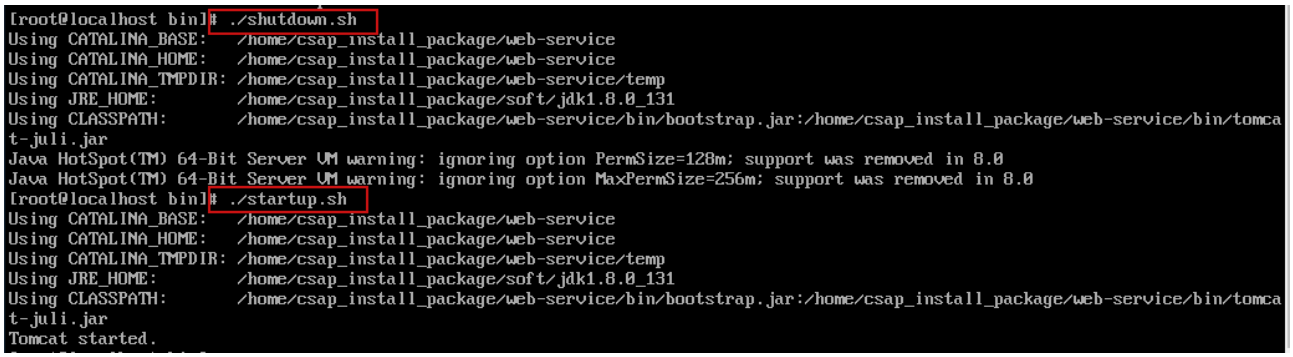
执行 ps –ef | grep tomcat 查找 tomcat 进程，然后执行 kill -9 id 终止该 id 进程

再次查找 tomcat 进程，直到进程数为 1 条时，则说明 tomcat 已全部终止。



执行./shutdown.sh

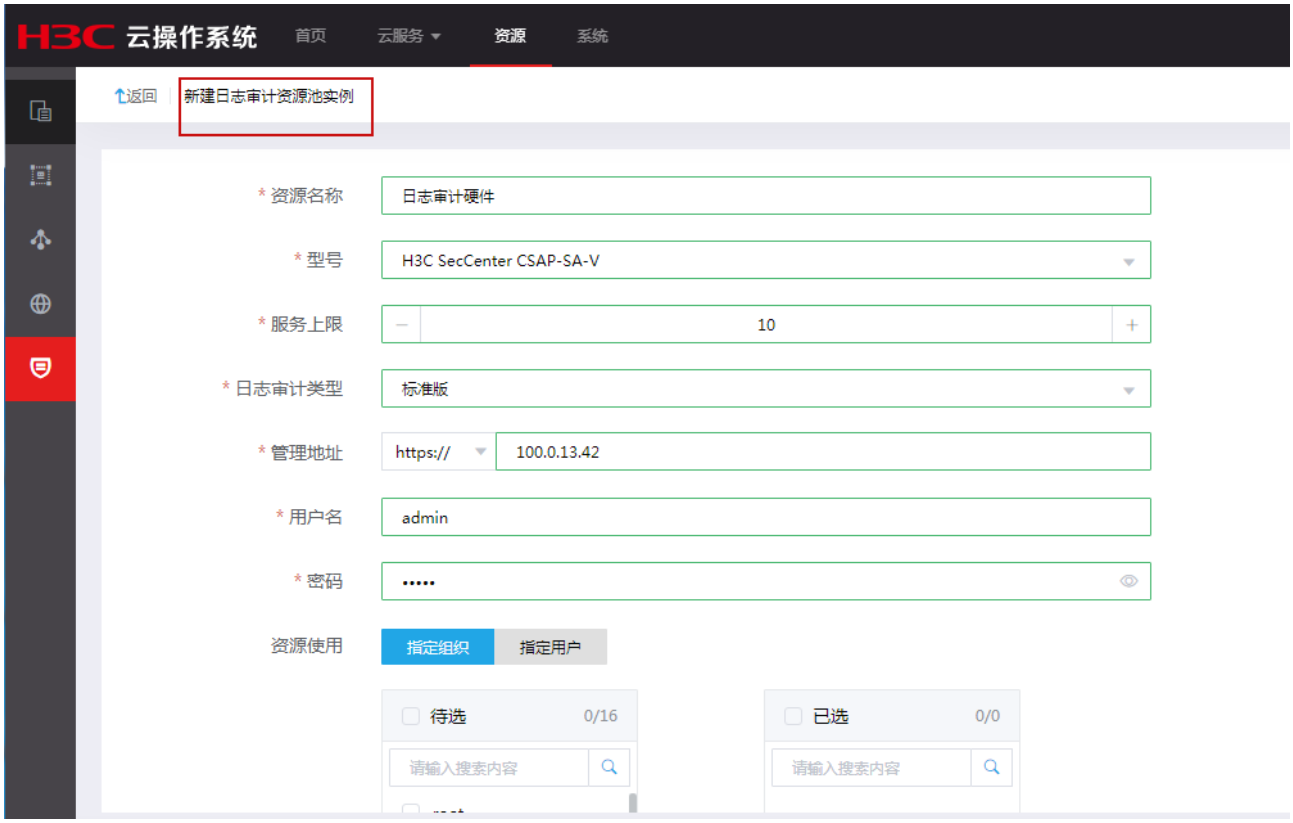
./startup.sh



(2) 添加日志审计资源

以云平台地址 100.0.13.105 为例，浏览器 URL 访问 http://100.0.13.105，使用系统管理员用户名/密码：admin/cloudos（具体以实际情况为准）登录云操作系统。单击[资源/安全资源池/日志审计资源池]菜单项，单击新建，填写必填的参数，URL 为日志审计设备地址，格式为“http://*ip*”。服务上限的意义是当输入服务上限，如服务上限为 3，则租户最多创建 3 个日志审计服务作用于当前添加的日志审计资源池。当选择指定组织/用户，则只有选中的组织/用户可以登录系统创建日志审计服务。日志审计资源类型为资源规格设置的类型。

图3-8 添加日志审计资源



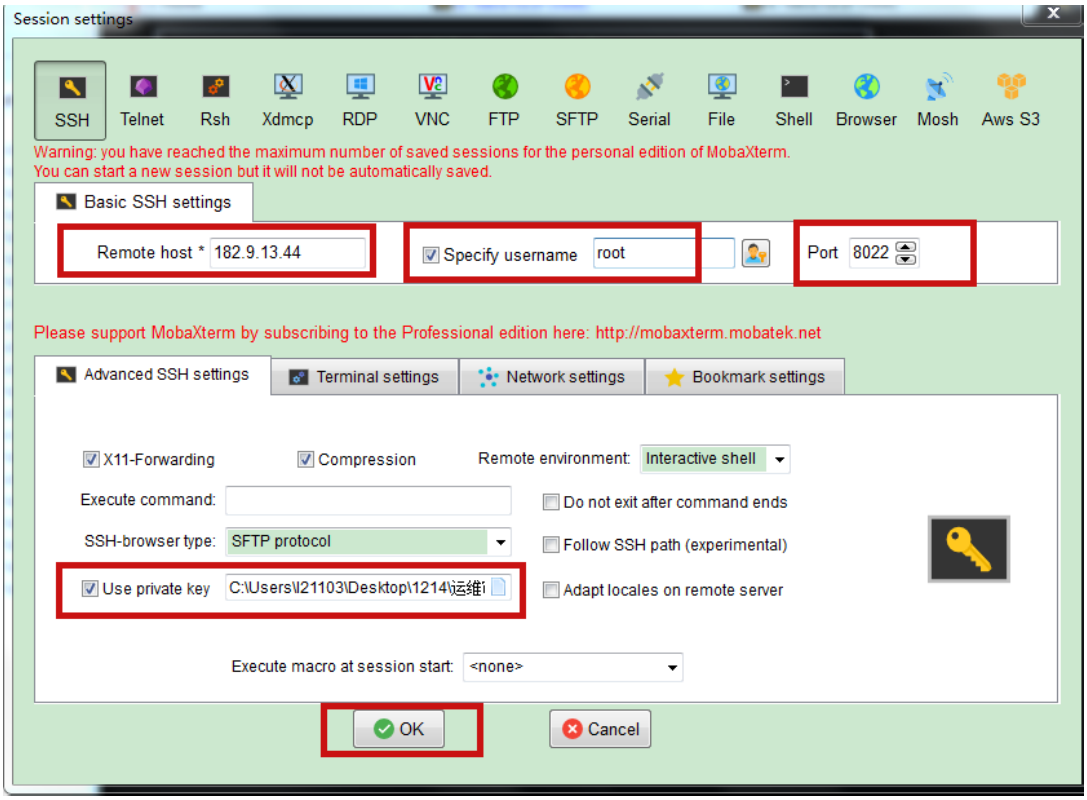
2. 堡垒机资源池

(1) 堡垒机资源准备

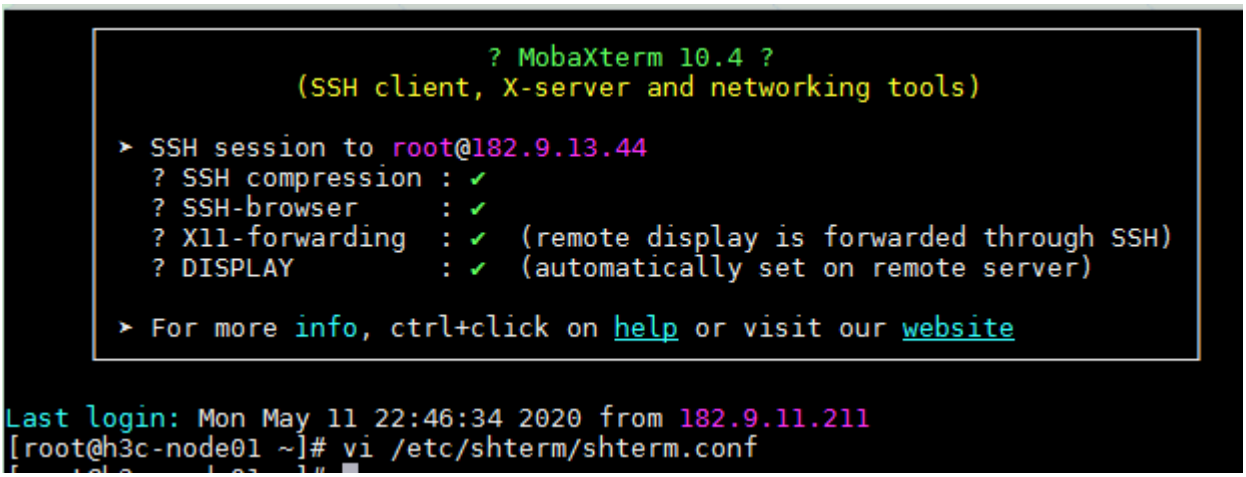
部署堡垒机服务，形式可以为硬件堡垒机服务或虚机堡垒机服务，具体版本要求见**错误!未找到引用源。**。

1）硬件堡垒机单点登录配置

通过秘钥登录硬件堡垒机后台



添加跳转重定向：vi /etc/shterm/shterm.conf 在配置里面添加： referer.accept=secaas。使之能够跳到运维审计系统，并重启 tomcat(systemctl restart tomcat)

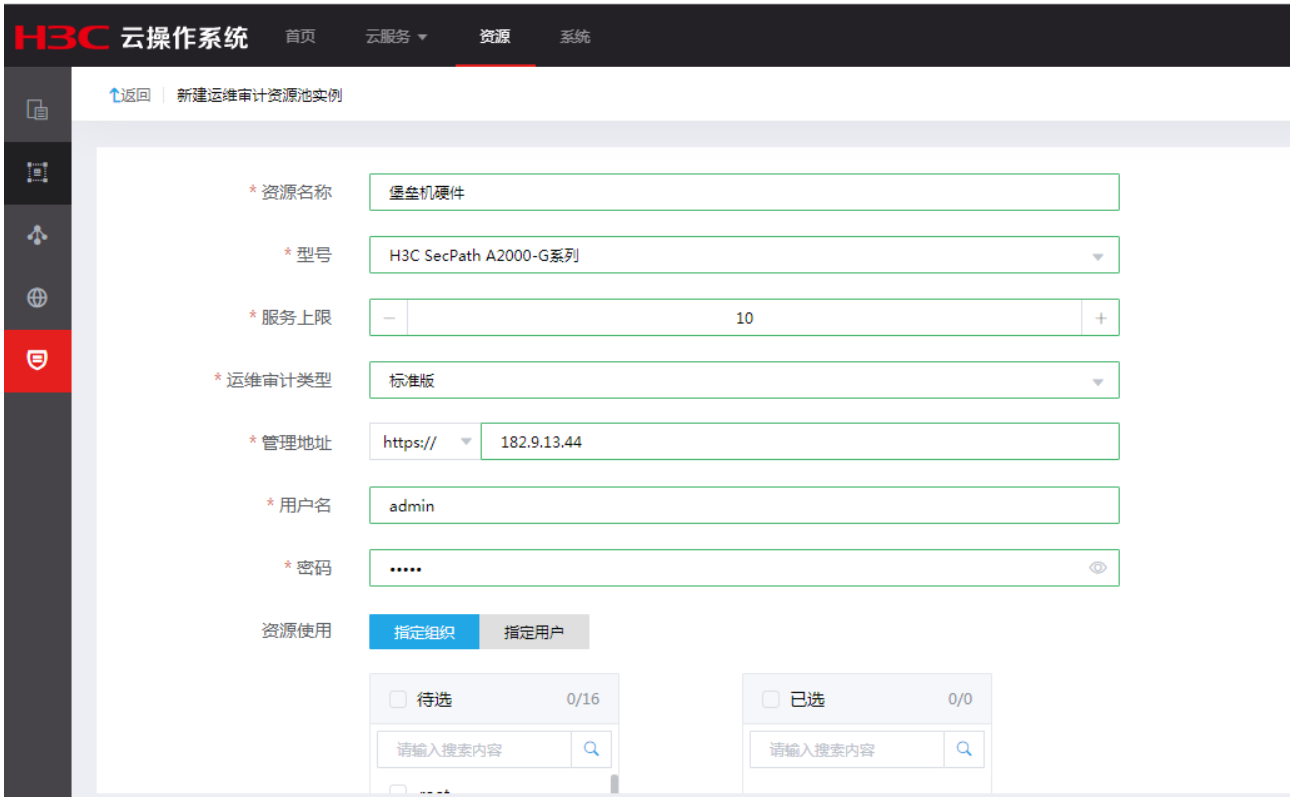


```
server.addr=localhost
db.url=jdbc:postgresql://${server.addr}/shterm
db.username=shterm
db.password=shterm
hibernate.showSql=false
hibernate.formatSql=false
amqp.addresses=${server.addr}
amqp.username=shterm
amqp.password=shterm
shterm.datadir=/var/shtermdata
health.red.exp=false
health.yellow.exp=false
referer.accept=secaas
~
~
```

2）添加堡垒机资源

以云平台地址 100.0.13.105 为例，浏览器 URL 访问 http://100.0.13.105，使用系统管理员用户名/密码：admin/cloudos（具体以实际情况为准）登录云操作系统。单击[资源/安全资源池/堡垒机资源池]菜单项，单击新建，填写必填的参数，其中管理员用户名、密码为登录堡垒机系统的用户名、密码，根据实际情况填写；URL 为堡垒机系统的访问地址，格式为 https://ip；服务上限的意义是当输入服务上限，如服务上限为 3，则租户最多创建 3 个堡垒机服务作用于当前添加的堡垒机资源池。当选择指定组织/用户，则只有选中的组织/用户可以登录系统创建堡垒机服务。堡垒机类型为资源规格设置的类型。

图3-9 添加堡垒机资源



3. 数据库审计资源池

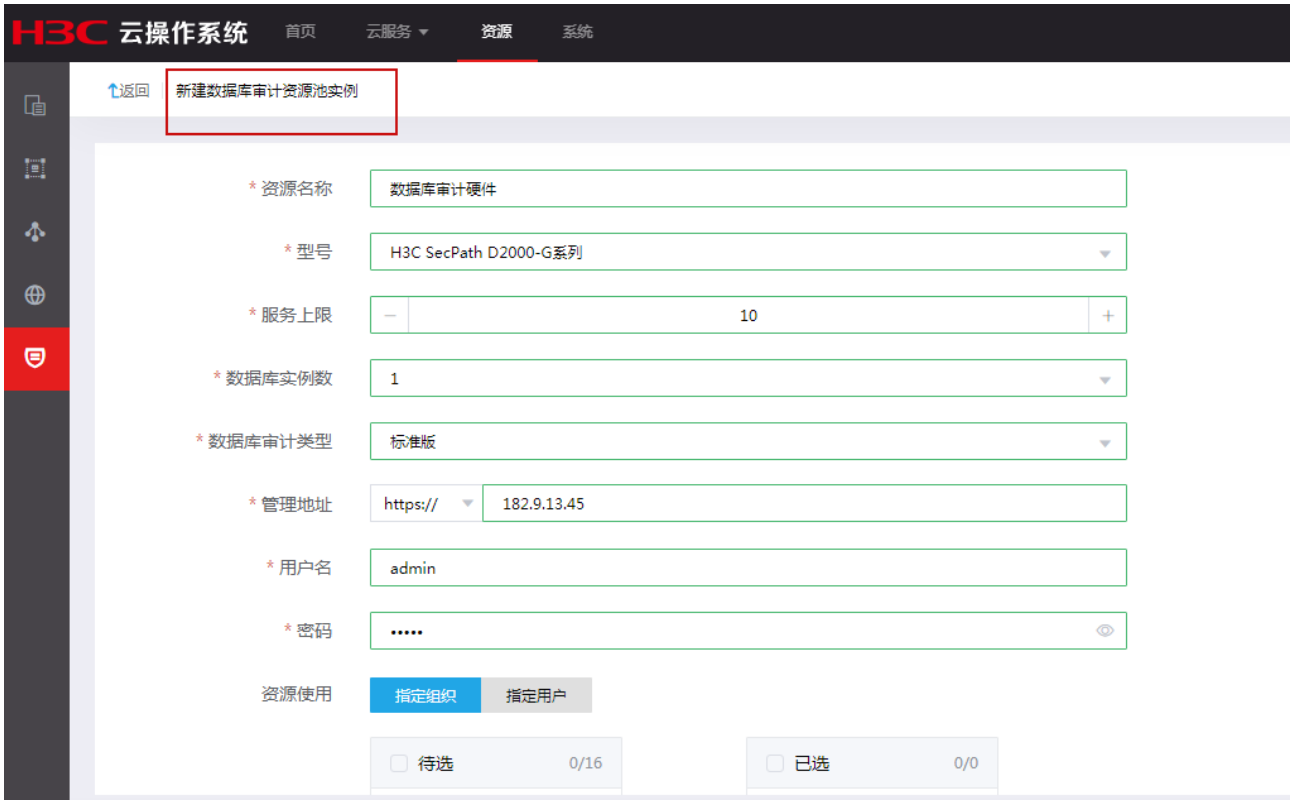
(1) 数据库审计资源准备

部署数据库审计服务，形式可以为硬件数据库审计服务或虚机数据库审计服务，具体版本要求请参见**错误!未找到引用源。**。请确保数据库审计系统时间与云操作系统服务器时间相差不超过 5 分钟。

(2) 添加数据库审计资源

以云平台地址 100.0.13.105 为例，浏览器 URL 访问 http://100.0.13.105，使用系统管理员用户名/密码：admin/cloudos（具体以实际情况为准）登录云操作系统。单击[资源/安全资源池/数据库审计资源池]菜单项，单击新建，填写必填的参数，其中管理员用户名、密码为登录数据库系统的用户名密码，URL 为数据库审计系统地址，格式为“http://*ip*”。服务上限的意义是当输入服务上限，如服务上限为 3，则租户最多创建 3 个数据库审计服务作用于当前添加的数据库审计资源池。当选择指定组织/用户，则只有选中的组织/用户可以登录系统创建数据库审计服务。数据库审计类型和数据库实例数为资源规格设置的值。

图3-10 添加数据库审计资源



4. 漏洞扫描资源池

(1) 漏洞扫描资源准备

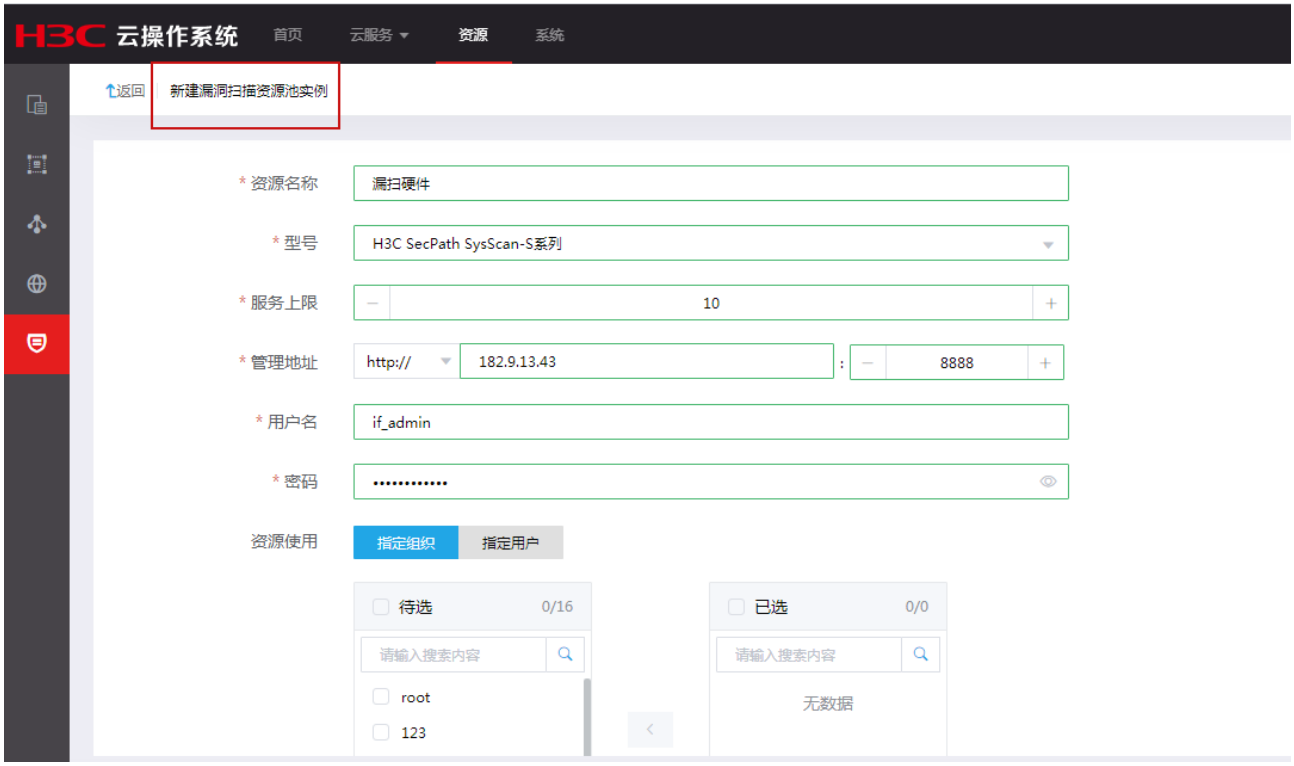
部署漏扫服务，形式可以为硬件漏扫服务或虚机漏扫服务，具体版本要求请参见**错误!未找到引用源。**。

(2) 添加漏洞扫描资源

以云平台地址 100.0.13.105 为例，浏览器 URL 访问 http://100.0.13.105，使用系统管理员用户名/密码：admin/cloudos（具体以实际情况为准）登录云操作系统。单击[资源/安全资源池/漏洞扫描

资源池]菜单项，单击新建，填写必填的参数，其中管理员用户名、密码并非登录漏扫系统的用户名密码，而是漏扫服务相关接口的用户名、密码，默认为 if_admin/if_admin@123，URL 为漏扫服务地址，格式为“http:///*ip:8888*”。服务上限的意义是当输入服务上限，如服务上限为 3，则租户最多创建 3 个漏扫服务作用于当前添加的漏扫资源池。当选择指定组织/用户，则只有选中的组织/用户可以登录系统创建漏扫服务。

图3-11 添加漏洞扫描资源



5. 应用监控资源池

(1) 应用监控资源准备

部署应用监控，形式可以为硬件应用监控服务或虚机应用监控服务，具体版本要求请参见**错误!未找到引用源。**。部署结束后，需要升级补丁应用监控补丁包，补丁包可从研发获取，补丁升级方式如下：

在应用监控路由可达的 FTP 服务器，补丁包放置在该 FTP 服务器中

1、 admin/admin 进入应用监控后台

2、 使用 sigup 命令升级

FTP 无用户名/密码： sigup ftp://ip/xxx.img

FTP 有用户名/密码: sigup ftp://user:password@ip/xxx.img

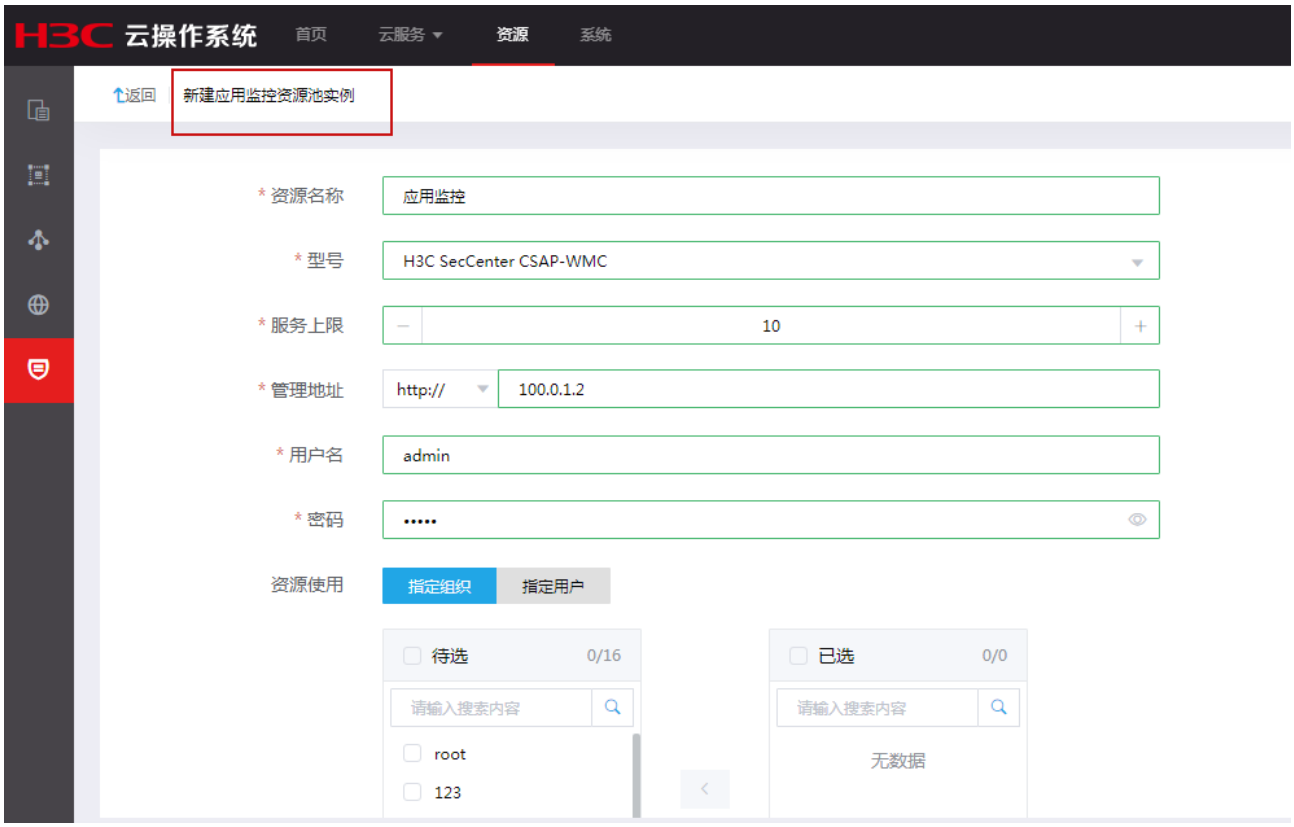
升级成功界面如下：

```
[h3c-os]$ sigup ftp://gyl:1@180.8.1.55:21/patch_h3c_bug_API.img
Fetch img file...
Decrypt img...
Update signature...
Using CATALINA_BASE:   /rayos/app/tomcat
Using CATALINA_HOME:   /rayos/app/tomcat
Using CATALINA_TMPDIR: /rayos/app/tomcat/temp
Using JRE_HOME:        /rayos/tools/jre
Using CLASSPATH:       /rayos/app/tomcat/bin/bootstrap.jar
Killing: 5363
Using CATALINA_BASE:   /rayos/app/tomcat
Using CATALINA_HOME:   /rayos/app/tomcat
Using CATALINA_TMPDIR: /rayos/app/tomcat/temp
Using JRE_HOME:        /rayos/tools/jre
Using CLASSPATH:       /rayos/app/tomcat/bin/bootstrap.jar
$CATALINA_PID was set (/rayos/app/tomcat/bin/CATALINA_PID) but the specified fil
e does not exist. Is Tomcat running? Stop aborted.
Using CATALINA_BASE:   /rayos/app/tomcat
Using CATALINA_HOME:   /rayos/app/tomcat
Using CATALINA_TMPDIR: /rayos/app/tomcat/temp
Using JRE_HOME:        /rayos/tools/jre
Using CLASSPATH:       /rayos/app/tomcat/bin/bootstrap.jar
update patch bug_3.0.1-R1-v32564 success!
[h3c-os]$
```

(2) 添加应用监控资源

以云平台地址 100.0.13.105 为例，浏览器 URL 访问 http://100.0.13.105，使用系统管理员用户名/密码：admin/cloudos（具体以实际情况为准）登录云操作系统。单击[资源/安全资源池/应用监控资源池]菜单项，单击新建，填写必填的参数，其中管理员用户名、密码为登录应用监控系统的用户名、密码，根据实际情况填写；URL 为应用监控服务地址，格式为“http://*ip*”。服务上限的意义是当输入服务上限，如服务上限为 3，则租户最多创建 3 个应用监控服务作用于当前添加的应用监控资源池。当选择指定组织/用户，则只有选中的组织/用户可以登录系统创建应用监控服务。

图3-12 添加应用监控资源



6. DDOS 资源池

(1) DDOS 防护资源准备

部署 DDOS 防护服务，形式为硬件 DDOS 防护服务，安全云对接的部署模式分为：旁路清洗，串联清洗，旁路清洗+检测，可根据局点现场 DDOS 部署模式在资源池中添加对应的实例，具体版本要求请参见**错误!未找到引用源。**。

登录 DDOS 设备 183.1.1.32（admin/admin），部署方式为旁路清洗，设置防御配置/全局参数，CC 防护开启时，状态监控》主机设置。主机设置中勾选 WEB Service Protection 防护插件；TCP 端口保护（端口保护设置集为 15，默认端口 0-65535）处协议选择 HTTP，防护模式勾选接受协议，防护插件选择 WEB Service Protection；CC 防护关闭时，状态监控》主机设置，相应的防护 IP-防护插件的 WEB Service Protection 为取消勾选，TCP 端口保护（端口保护设置集为 14，默认端口 0-65535）处对应的参数为空。

图3-13 配置 DDOS 防护参数（端口保护设置集为 15）

(2) 添加 DDOS 防护资源

以云平台地址 100.0.13.105 为例，浏览器 URL 访问 http://100.0.13.105，使用系统管理员用户名/密码：admin/cloudos（具体以实际情况为准）登录云操作系统。单击[资源/安全资源池/DDOS 防护资源池]菜单项，单击新建，填写必填的参数，其中管理员用户名、密码为登录 DDOS 设备的用户名密码，URL 为 DDOS 设备地址，格式为“http://ip”。服务上限的意义是当输入服务上限，如服务上限为 3，则租户最多创建 3 个 DDOS 防护服务作用于当前添加的 DDOS 防护资源池。当选择指定组织/用户，则只有选中的组织/用户可以登录系统创建 DDOS 防护服务。

单击[资源/安全资源池/DDOS 防护资源池]菜单项，单击操作列的防御配置，配置防御配置各参数，系统管理员可以设置系统操作环境、系统防护参数、主机防护参数。

图3-14 添加 DDOS 防护资源

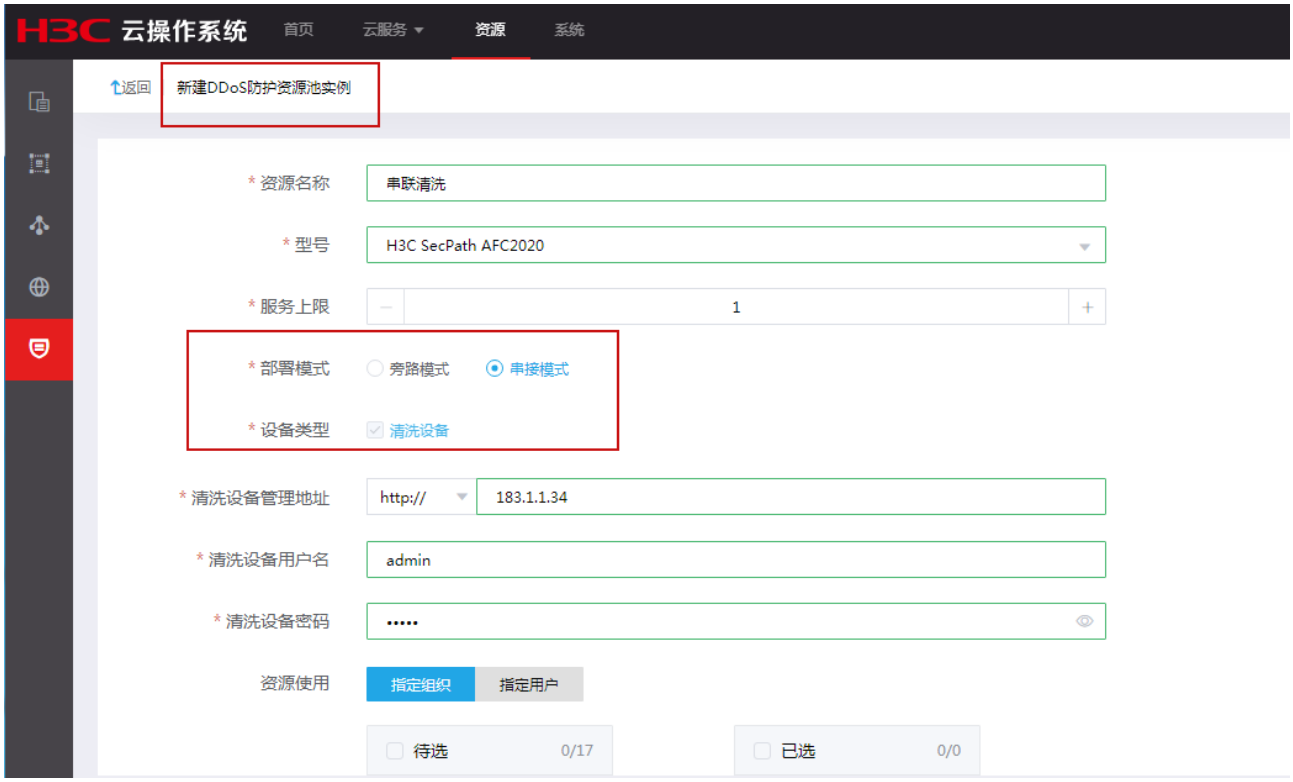


图3-15 DDOS 防御参数配置 （旁路清洗）

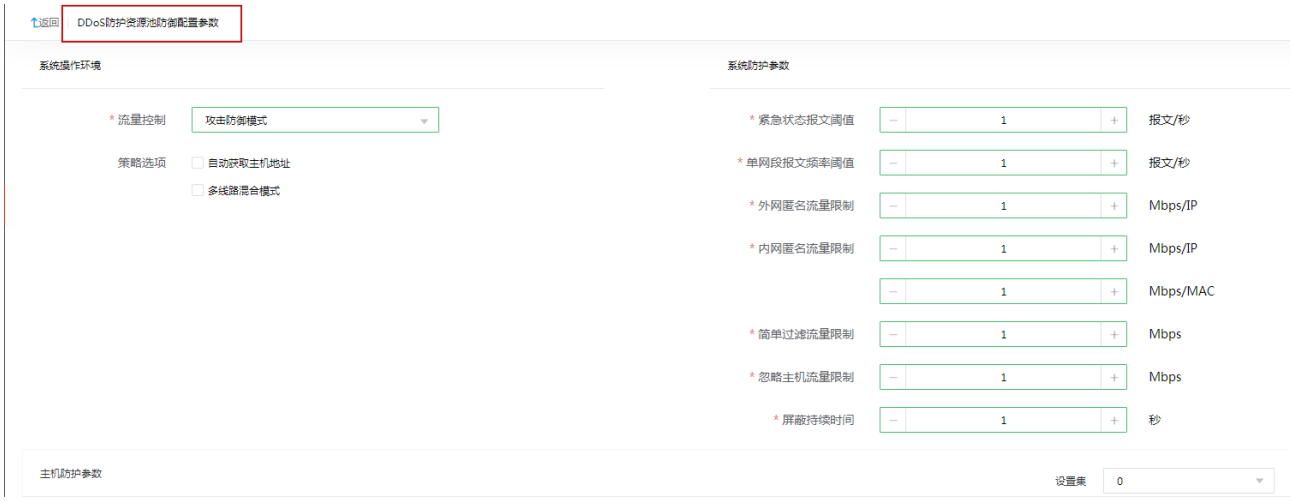
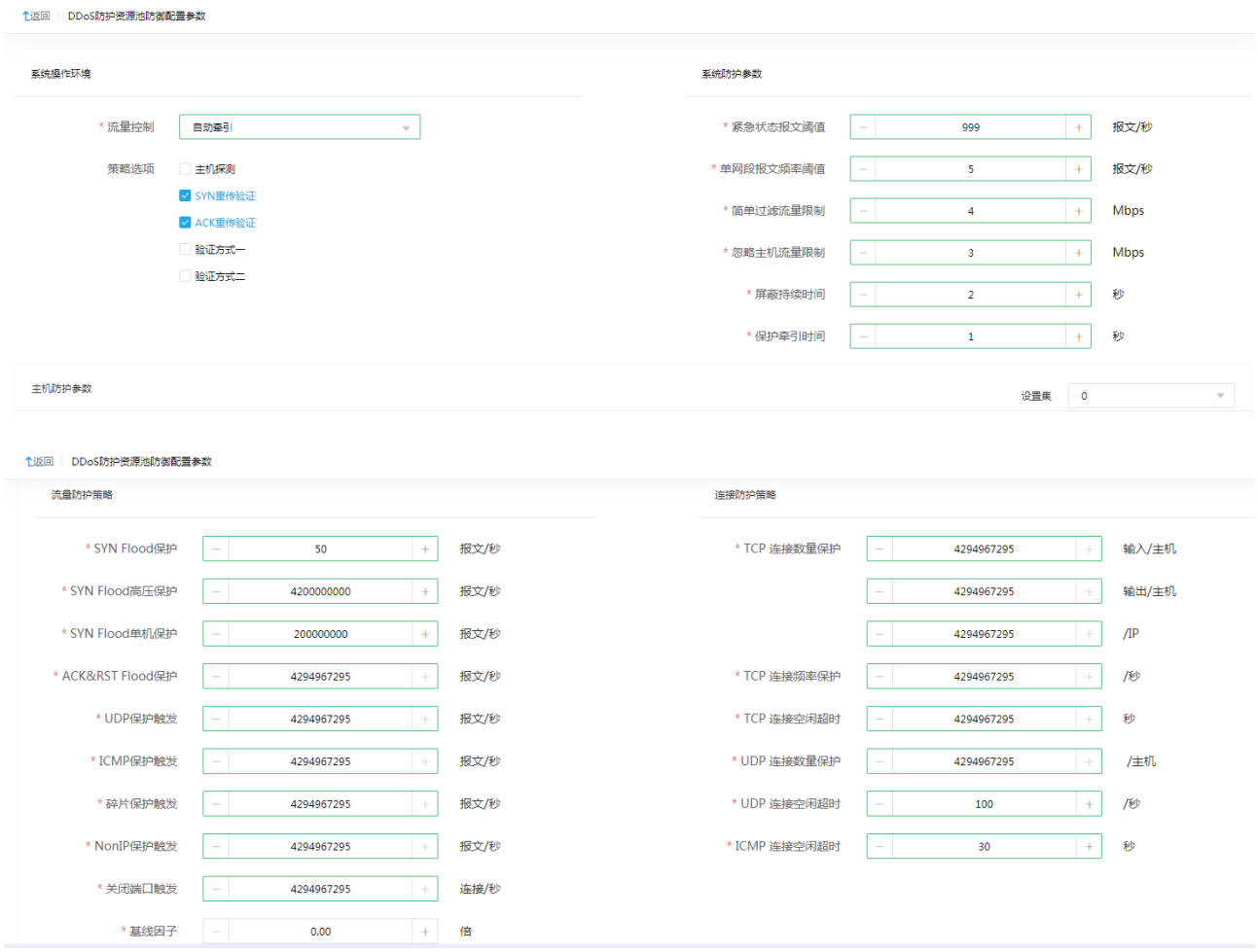


图3-16 DDOS 防御参数配置 （串联清洗）



7. Web 应用防护资源池

(1) Web 应用防护资源准备

1）部署 Web 应用防护服务，形式为云 Web 应用防护服务，具体版本要求请参见[错误!未找到引用源。。](#)添加两个网卡，一个为管理网卡 port0，一个为业务网卡 port1。

2）WAF 设备网络管理——网桥接口配置接口名称为 66 的网桥接口（注意网桥号填写 66），并在业务网 port1 接口中绑定该网桥接口；

图3-17 创建网桥 br66

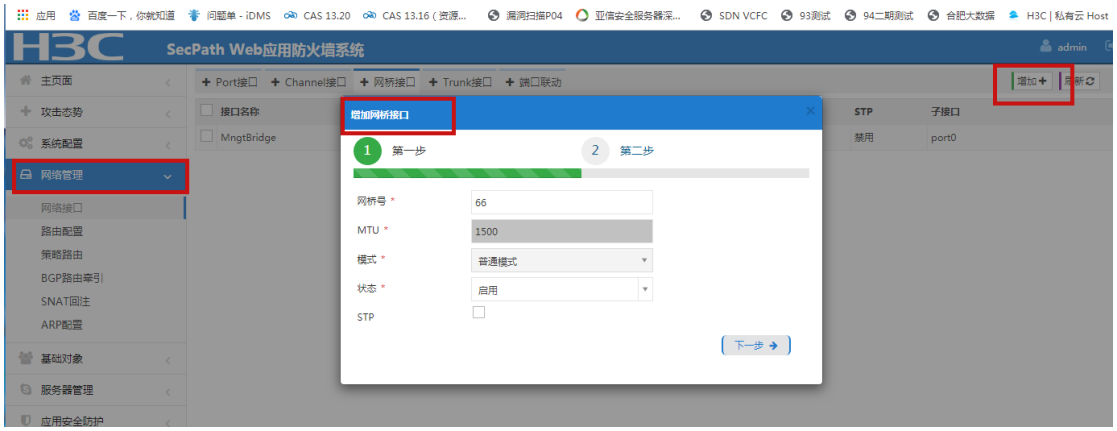
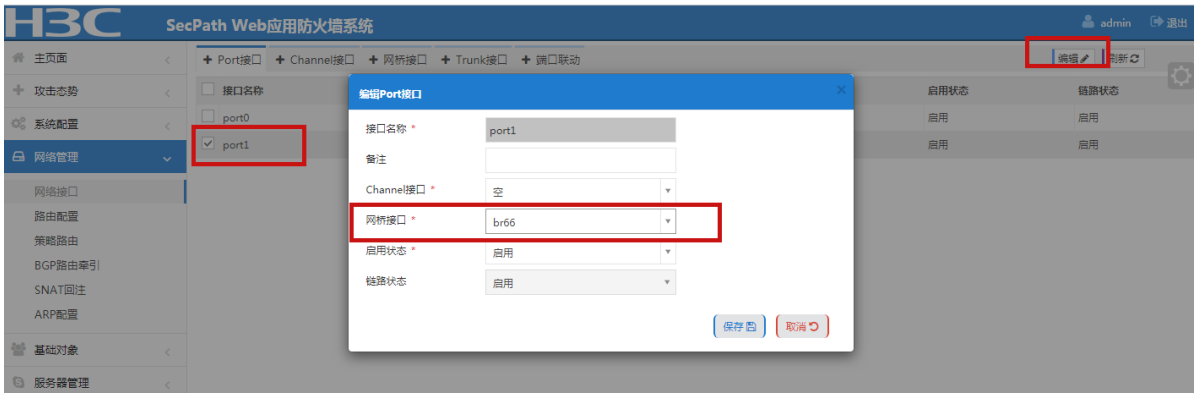
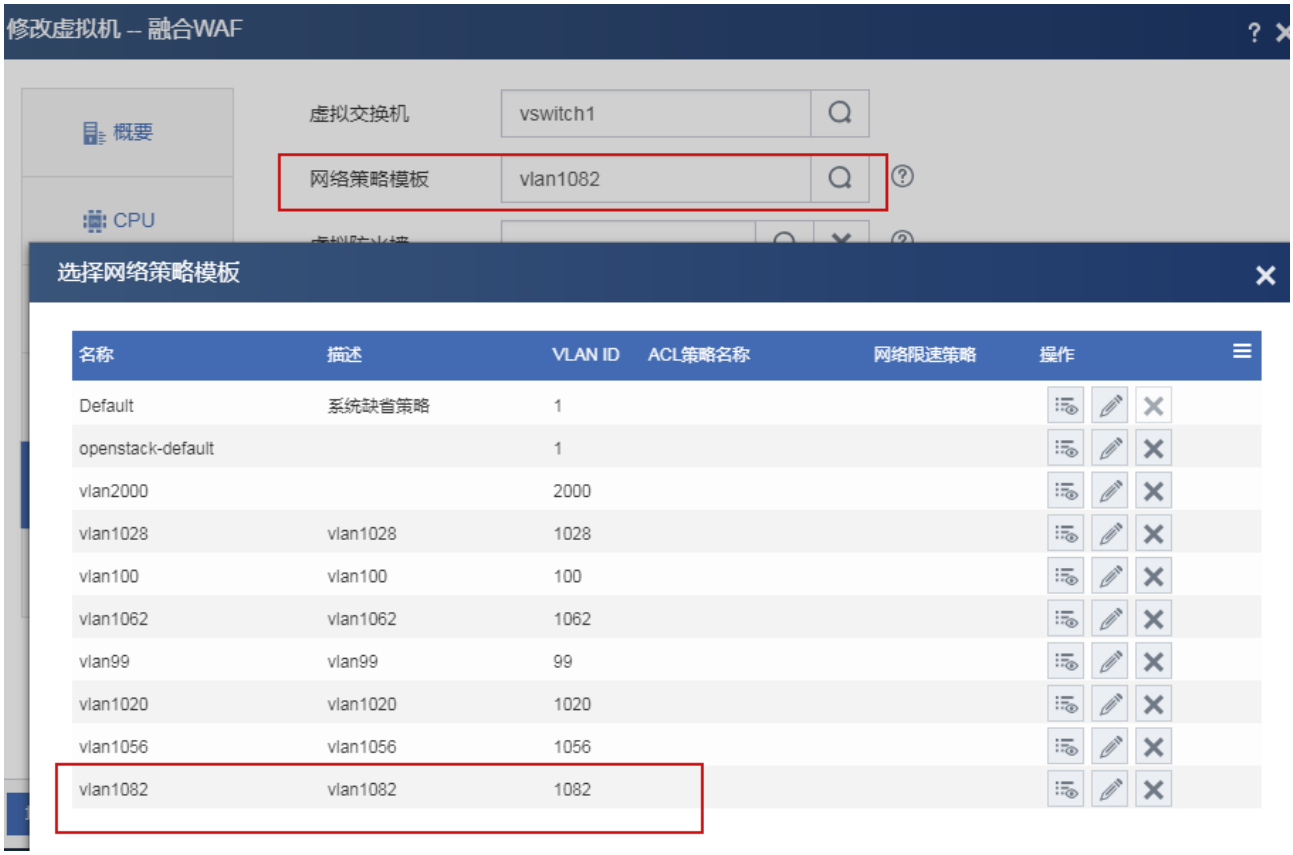


图3-18 绑定网桥接口



3）在 CAS 中手动配置业务口网络策略模板，其中的网络策略模板 VLAN 需要与租户经典网络的 VLAN 信息一致。

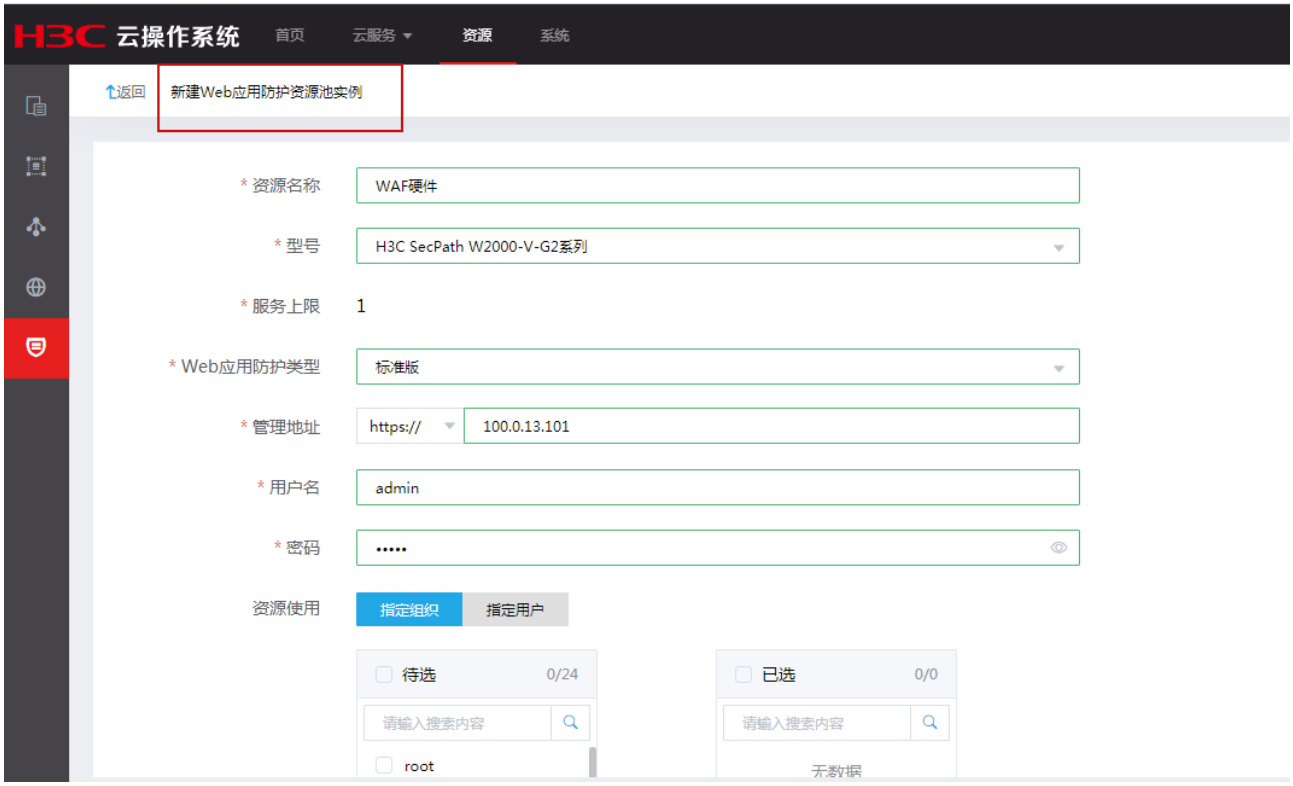
图3-19 网络策略模板配置



(2) 添加 Web 应用防护资源

以云平台地址 100.0.13.105 为例，浏览器 URL 访问 http://100.0.13.105，使用系统管理员用户名/密码：admin/cloudos（具体以实际情况为准）登录云操作系统。单击[资源/安全资源池/Web 应用防护资源池]菜单项，单击新建，填写必填的参数，其中管理员用户名、密码为登录 Web 应用防护系统的用户名密码，URL 为 Web 应用防护系统地址，格式为“https://*ip*”。Web 应用防护目前不支持共享，一个安全资源对应一个安全服务。当选择指定组织/用户，则只有选中的组织/用户可以登录系统创建 Web 应用防护服务。Web 应用防护类型为资源规格设置的类型。

图3-20 添加 Web 应用防护资源



8. 服务器安全监测资源池

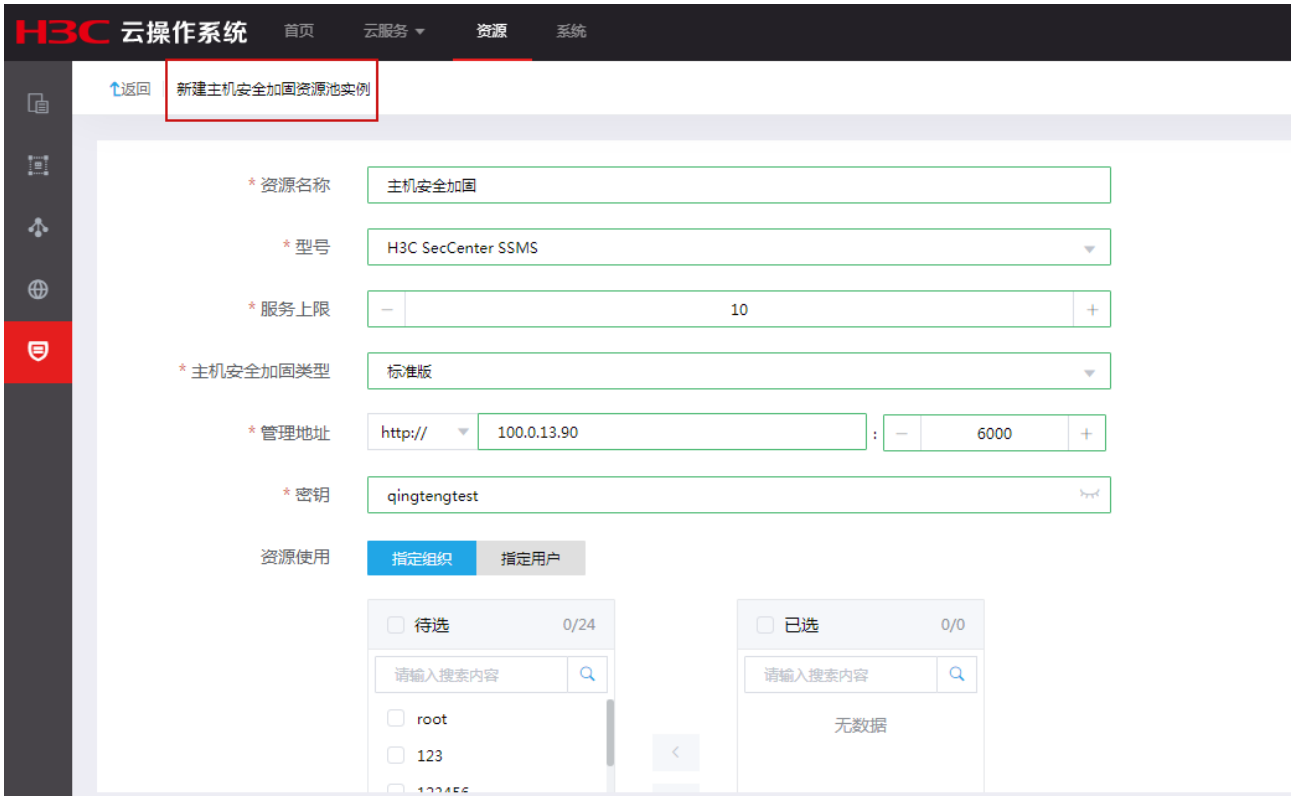
(1) 服务器安全监测资源准备

部署服务器安全监测服务，以青藤安全为例：在 CAS 部署服务器安全监测虚拟机，启动虚拟机。访问 https://ServerIP:82（ServerIP 指目标服务器的 IP 地址，例如：https://100.0.13.90:82），进入“系统配置管理”的登录界面，用户名/密码：admin/admin。

(2) 添加服务器安全监测资源

以云平台地址 100.0.13.105 为例，浏览器 URL 访问 http://100.0.13.105，使用系统管理员用户名/密码：admin/cloudos（具体以实际情况为准）登录云平台。单击[资源/安全资源池/服务器安全监测资源池]菜单项，单击新建，填写管理地址，格式为“http://ip:6000”，秘钥默认为 qingtengtest，填写必填信息。服务上限的意义是当输入服务上限，如服务上限为 3，则最多允许 3 个租户创建服务器安全监测服务作用于当前添加的服务器安全监测资源池。当选择指定组织/用户，则只有选中的组织/用户可以登录系统创建服务器安全监测服务。

图3-21 添加服务器安全监测资源



9. 态势感知资源池

(1) 态势感知资源准备

1）部署态势感知服务，形式可以为硬件态势感知服务或虚机态势感知服务，具体版本要求请参见[错误!未找到引用源。]。

2）开启态势感知单点登录功能（root/csap_H3C@yunzhi）

图 4-23 为态势感知配置。

cd /opt/web-service/webapps/skynet/WEB-INF/classes/

vi configuration.properties

图3-22 访问态势感知后台

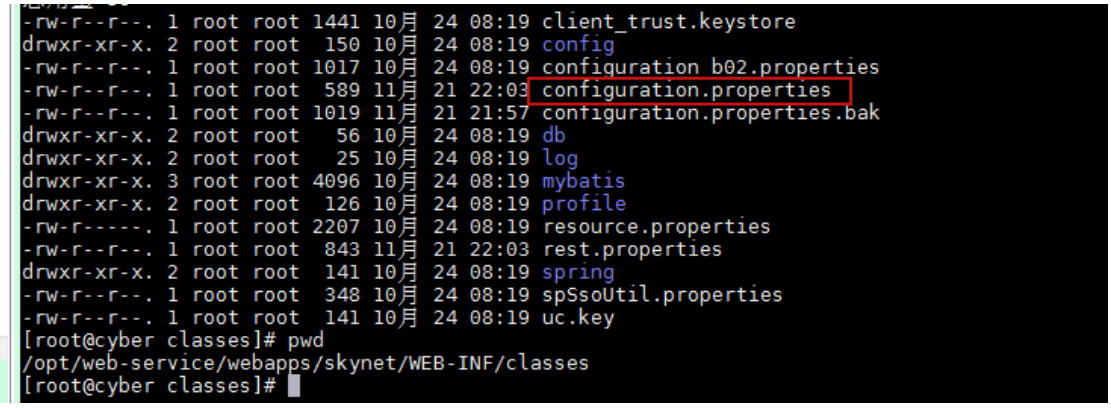
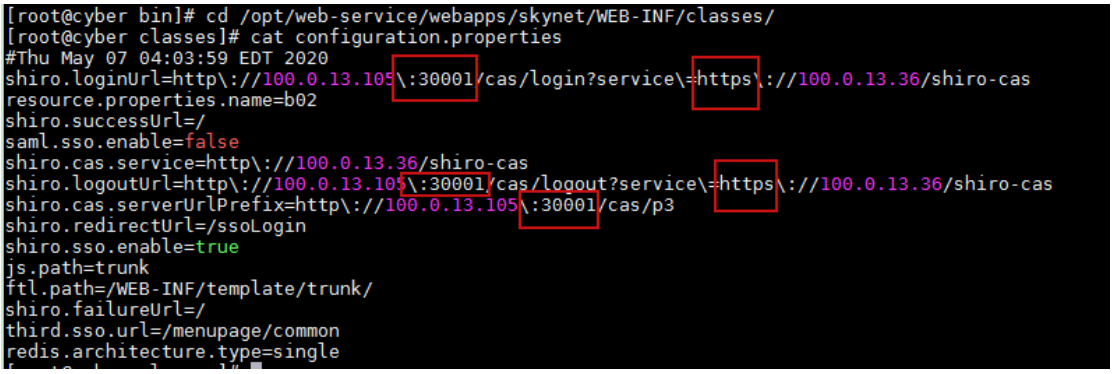


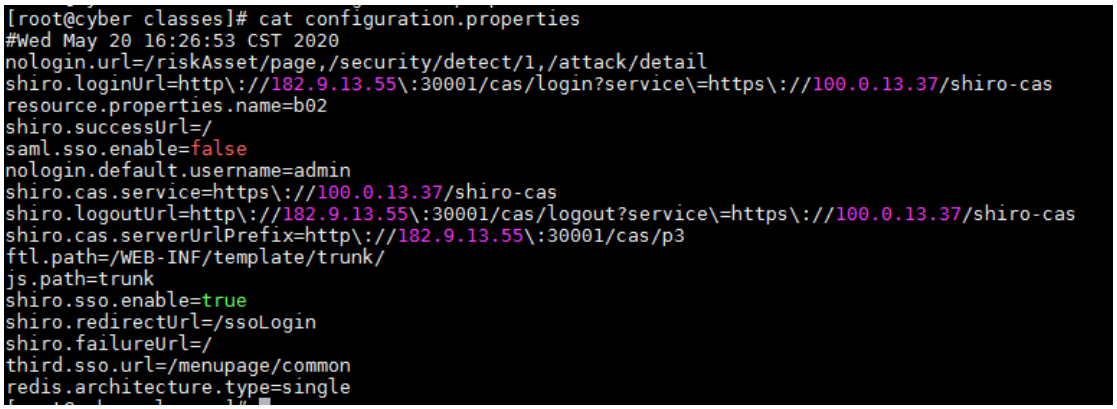
图3-23 配置态势感知



其中 100.0.13.36 为态势感知地址，100.0.13.105 为融合 5.0 地址。

图3-24 配置态势感知多租户版本

（182.9.13.55 为集群环境，100.0.13.37 为态势感知地址）



3）重启 tomcat 服务

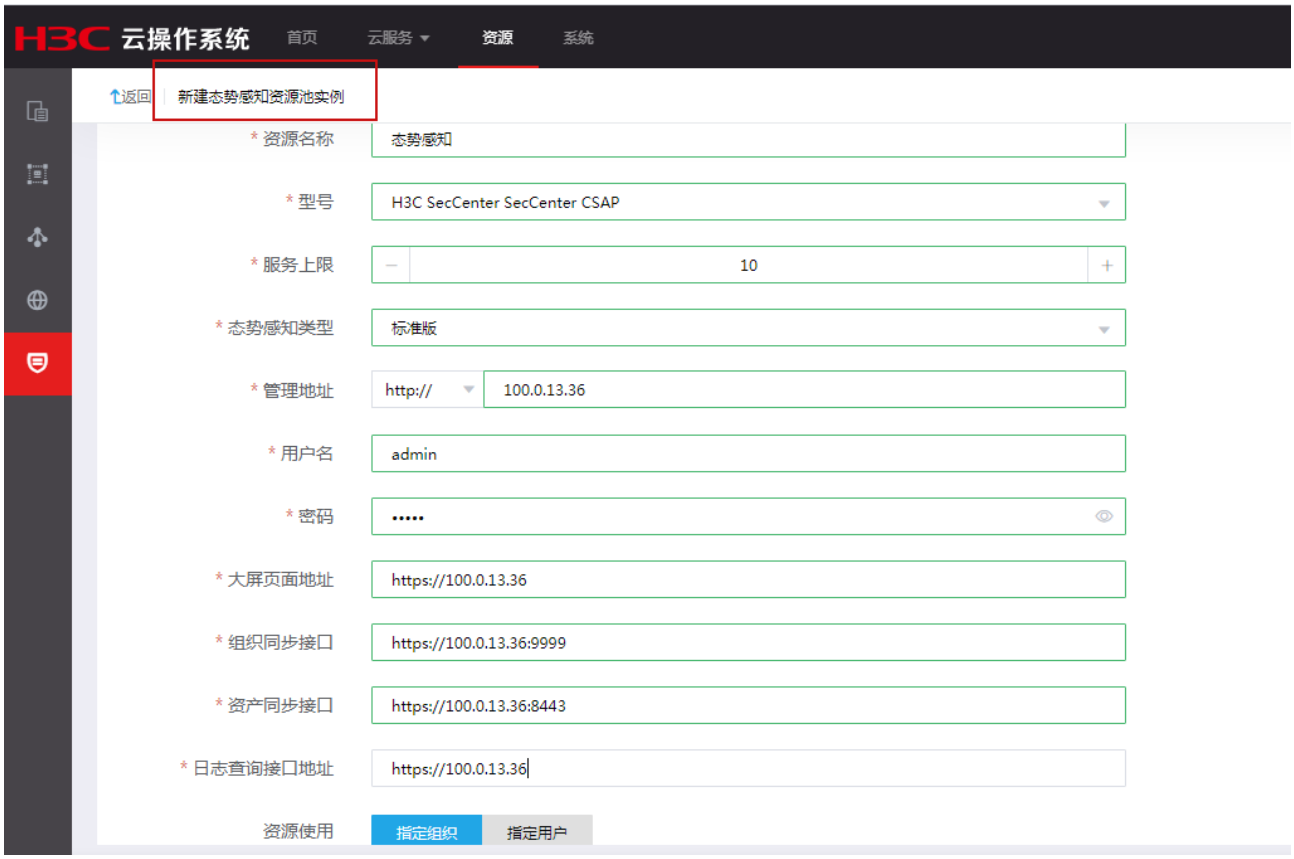
sh /opt/web-service/bin/shutdown.sh

sh /opt/web-service/bin/startup.sh

(2) 添加态势感知资源

以云平台地址 100.0.13.105 为例，浏览器 URL 访问 http://100.0.13.105，使用系统管理员用户名/密码：admin/cloudos（具体以实际情况为准）登录云平台。单击[资源/安全资源池/态势感知资源池]菜单项，单击新建，填写管理地址、大屏页面地址、组织同步接口、资产同步接口等必填信息。服务上限的意义是当输入服务上限，如服务上限为 3，则最多允许 3 个租户创建态势感知服务作用于当前添加的态势感知资源池。当选择指定组织/用户，则只有选中的组织/用户可以登录系统创建态势感知服务。

图3-25 添加态势感知资源



3.3 分配配额

配额为创建服务所需资源，需要云管理员根据安全资源能力进行统一规划并分配给租户使用，使租户可创建相应服务；

以云平台地址 100.0.13.105 为例，浏览器 URL 访问 http://100.0.13.105，使用系统管理员用户名/密码：admin/cloudos（具体以实际情况为准）登录云操作系统。点击[系统/组织管理/配额]选择相应的组织或者用户，点击修改，可以给相应的用户或者组织分配配额。组织管理员登录云操作系统[组织/配额]选择本组织名称，或者组织下用户，点击配额，可以设置本组织，以及本组织内成员的安全配额值。

图3-26 给组织分配配额（系统管理员）

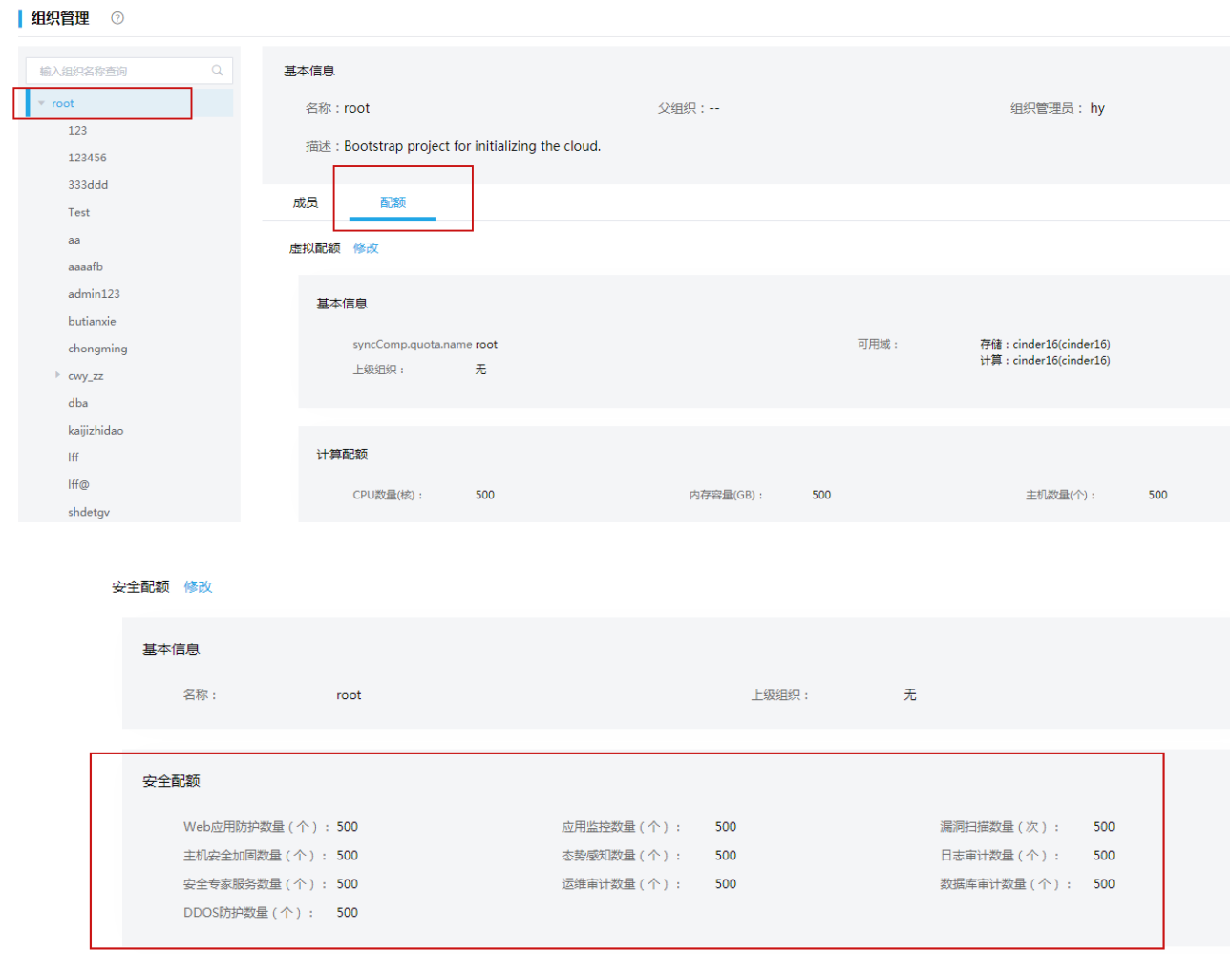
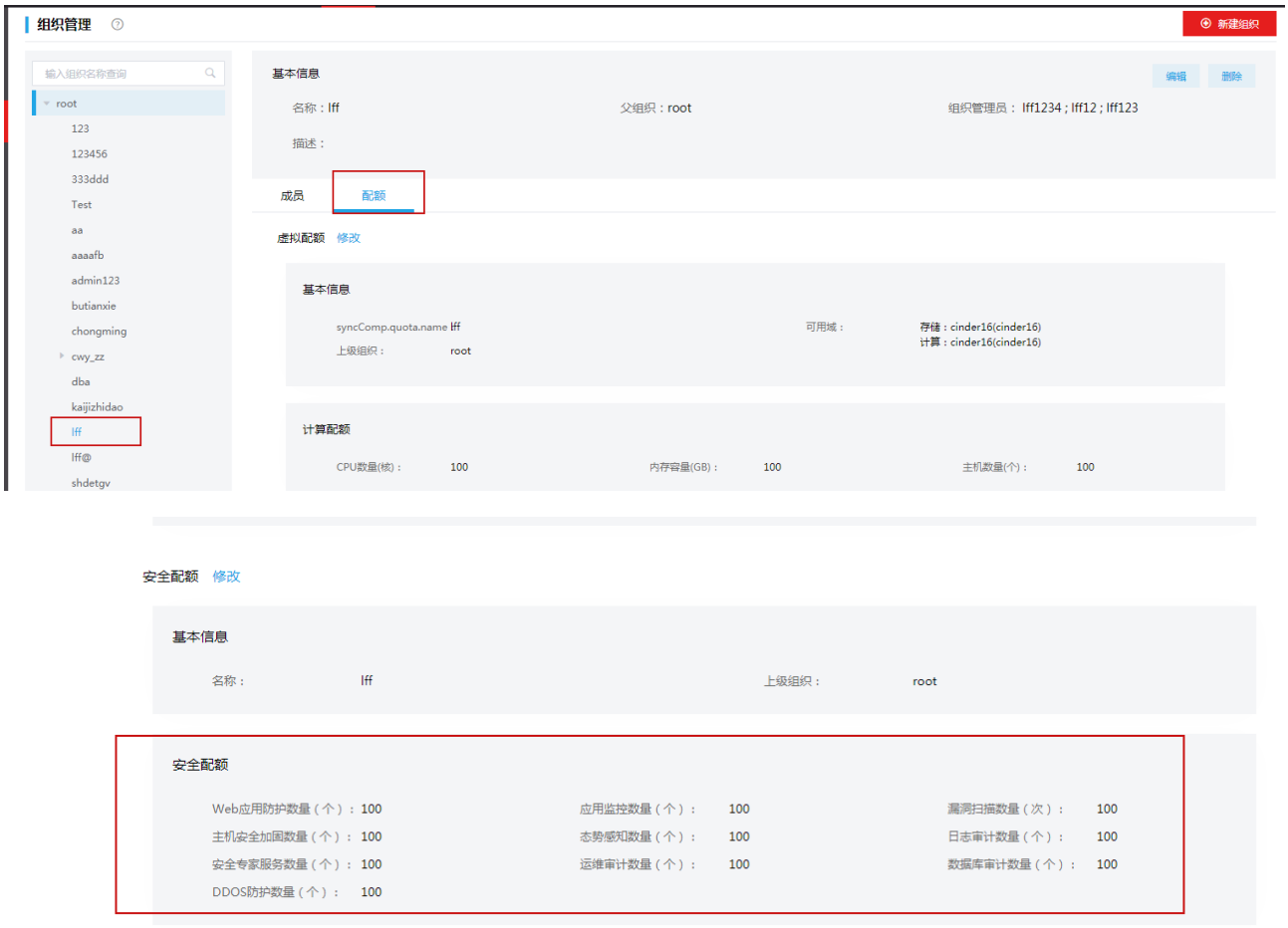


图3-27 分配配额（组织）



3.4 设置资源规格

资源规格的设置便于对安全服务下发计费策略，不同规格服务可设置不同的计费策略。若不存在计费需求可不设置。

以云平台地址 100.0.13.105 为例，浏览器 URL 访问 http://100.0.13.105，使用系统管理员用户名/密码：admin/cloudos（具体以实际情况为准）登录云操作系统。以新建应用监控资源规格为例。单击[云服务/应用监控/服务配置]菜单项，点击新建，选择不同的值，建立不同的规格类型。

图3-28 设置资源规格

3.5 普通用户申请服务

普通用户角色可申请 Web 应用防护、应用监控、漏洞扫描、DDOS 防护四种安全服务，以漏扫为例，讲解普通用户申请安全服务流程。普通用户登录云平台，单击[云服务-漏洞扫描]，选择相应的漏洞扫描列表去申请漏扫扫描服务，如申请 Web 漏扫，单击申请，填写任务名称，扫描地址，选择策略模板，单击确定。普通用户每一条申请记录会生成流程记录，需要上一级组织管理员审批，组织管理员在流程处审批通过后，普通用户服务列表中会展示申请的服务，状态为正常运行。

图3-29 普通用户申请

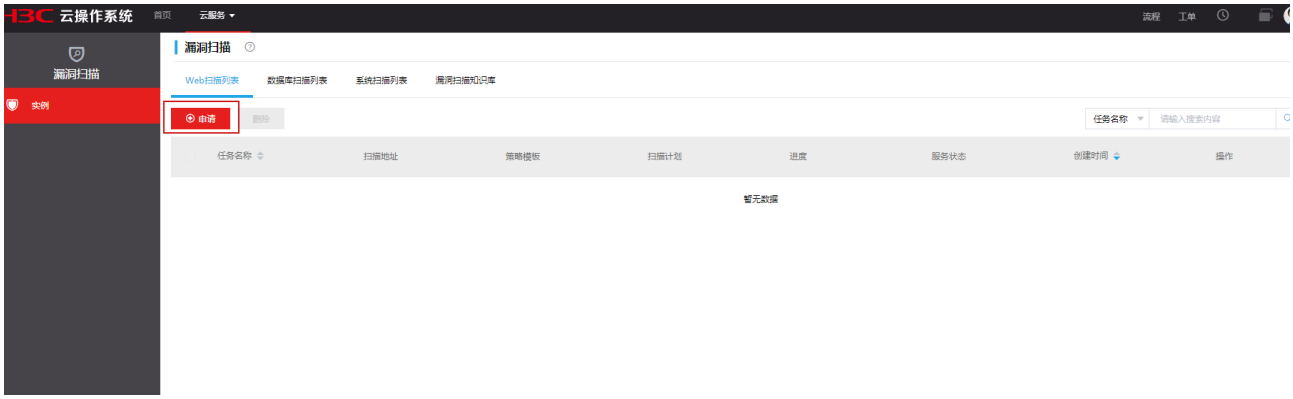


图3-30 普通用户申请

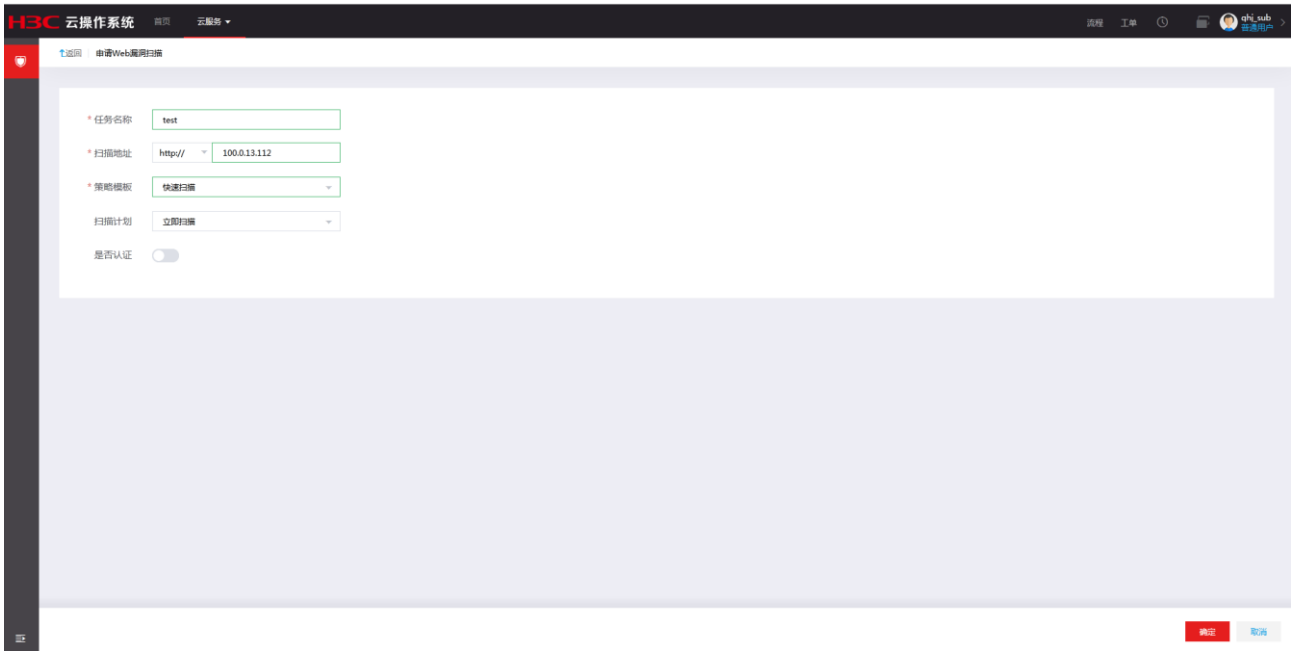


图3-31 普通用户流程列表

图3-32 组织管理员流程列表

图3-33 普通用户漏洞扫描列表