第3章

虚拟化安全

虚拟化安全管理系统是面向云计算或虚拟化环境的一站式安全产品。虚拟化安全利 用主机防火墙、IPS、多引擎病毒查杀等安全技术,实现从虚拟机资源池中的底层安全,到 虚拟机的系统安全,到虚拟机内部的应用安全的立体防御,为企业提供由外到内、自上至 下的运行环境。

虚拟化安全管理系统提供以下功能。

1) 恶意软件防护

虚拟化安全管理系统防恶意软件模块可提供防恶意软件防护,恶意代码包括:敲诈 勒索软件、病毒、蠕虫、木马后门等,包括实时扫描、预设扫描及手动扫描功能,处理措施包 含清除、删除、拒绝访问或隔离恶意软件。

2) 虚拟防火墙

虚拟化安全管理系统防火墙模块可用于启用正确的服务器运行所必需的端口和协议 上的通信,并阻止其他所有端口和协议,降低对服务器进行未授权访问的风险。

3) 入侵防御

虚拟化安全解决方案入侵防御模块能够对暴力破解、缓冲溢出、漏洞利用等网络攻击行为进行检测和拦截。

4) 主机加固

虚拟化安全管理系统对宿主机及虚拟机展开安全检查,找出不符合的项目并选择和 实施安全措施来控制安全风险。

5) Webshell 检测

虚拟化安全管理系统可对各种 Webshell 后门文件进行扫描与隔离,有效对主机进行 安全加固,抵御来自外来 Web 漏洞利用的攻击。

3.1 客户端安装与卸载

3.1.1 虚拟化安全管理系统 Linux 客户端安装及卸载实验

【实验目的】

完成虚拟化安全管理系统 Linux 客户端的部署。

【知识点】

虚拟化安全管理、Linux 客户端安装及卸载。

【场景描述】

A 公司虚拟化安全管理系统控制中心服务器部署完毕后,需要在虚拟化安全管理系统管理的主机中安装客户端程序。主机分为两种操作系统:Windows和 Linux。安全运维工程师小王需要为所辖 Linux 主机配置虚拟化安全管理系统客户端,熟悉客户端的安装、卸载流程,请帮助小王熟悉虚拟化安全管理系统 Linux 客户端的配置。

【实验原理】

管理员在 Linux 主机中通过执行下载命令从下载地址处下载虚拟化安全管理系统 Linux 客户端安装包,并进行安装。通过执行卸载命令,将虚拟化安全管理系统从 Linux 客户端删除。

【实验设备】

安全设备:云安全设备1台。 基础设施:安全云设备1台。 主机终端:Windows7主机1台。

【实验拓扑】

实验拓扑如图 3-1 所示。



图 3-1 虚拟化安全管理系统 Linux 客户端安装及卸载实验拓扑图

【实验思路】

(1) 登录云安全管理平台。

(2) 创建租户以及租户用户。

(3) 租户用户申请安全组件。

(4) 登录安全云平台,创建虚拟机。

(5) 下载安装虚拟化客户端。

(6) 卸载客户端。

【实验步骤】

1. 登录云安全平台

(1)登录实验平台对应实验拓扑左侧的管理机,进入管理机,打开浏览器,在地址栏 中输入云安全平台的 IP 地址"https://10.95.134.52"(以实际设备 IP 地址为准),进入云 安全平台的登录界面。输入系统管理员用户名密码"sysadmin/csmp@qihoo360"(以实际 用户名/密码为准),单击"立即登录"按钮,进入云安全平台。

(2) 登录云安全平台后,显示云安全平台的面板界面。

2. 新建租户以及租户用户

(1) 单击左侧"用户管理"按钮→单击"租户"按钮,进入租户管理界面。

(2) 在"租户"界面中,单击"+添加租户"按钮,添加一个租户。

(3) 在弹出的"添加租户"对话框中,填写"租户 ID"为 TechDepartment(由于并行操作人员可能较多,为避免命名冲突,建议使用学生个人名字进行命名),填写"租户名称"为"技术部",填写"描述"为"技术部",单击"保存"按钮,新建技术部租户。

(4) 返回"租户"界面,可以看到新建技术部租户成功。

(5) 单击"租户"名称为"技术部"列表右侧的"查看详情"按钮,查看该租户的详细信息。

(6)进入"技术部"租户界面,单击"十添加租户用户"按钮,为该租户添加一个用户, 如图 3-2 所示。

用户管理 / 租户 / 技术部 + 添加用户账号 批量場作 ×	Q					
用户账号	姓名	邮箱	手机	角色	状态	操作
TechDepartment_aud	租户审计管理员	-	-	租户审计管理员	• 正常	编辑
TechDepartment_sec	租户安全管理员	-	-	租户安全管理员	• 正常	编辑
TechDepartment_sys	租户系统管理员	-		租户系统管理员	• 正常	编辑
				共3条 10	<u>§</u> ∨ < 1 >	〕跳至 1

图 3-2 添加租户用户

(7) 在弹出的"添加租户用户"界面中,填写"账号"为 staff01,填写"姓名"为"王小明" (由于并行操作人员可能较多,为避免命名冲突,建议使用学生个人名字进行命名),填写 "密码"为 xiaoming,填写"确认密码"为 xiaoming,填写"邮箱"为"xiaoming@360.net",填 写"描述"为"技术部员工",单击"保存"按钮。

(8) 返回"技术部"租户界面,可以看到已成功新建租户用户,如图 3-3 所示。

(9) 单击界面上方"租户"按钮,返回"租户"界面,可以看到"技术部"租户下的"用户

用户管	理/租户/技术部						
+ 添	加用戶账号 批量操作 > 清報	輸入账号搜索 Q					
	用户账号	姓名	邮箱	手机	角色	状态	操作
	TechDepartment_aud	租户审计管理员	-	-	租户审计管理员	• 正常	編輯
	TechDepartment_sec	租户安全管理员	-	-	租户安全管理员	• 正常	编辑
	TechDepartment_sys	租户系统管理员	-	-	租户系统管理员	• 正常	编辑
	staff01	王小明		-	-	 - 锁定 	编辑:删除
					共4条	10条× < 1	> 跳至

图 3-3 新建租户用户成功

数"变为4,成功新建用户,如图 3-4 所示。

用户管	理/租户/技术部						
批量	₩操作 ~ 请输入账号搜索	Q					
	用户账号	姓名	邮箱	手机	角色	状态	操作
	TechDepartment_aud	租户审计管理员	-	-	租户审计管理员	• 正常	锁定:重置密码
	TechDepartment_sec	租户安全管理员	-	-	租户安全管理员	• 正常	锁定:重置密码
	TechDepartment_sys	租户系统管理员	-	-	租户系统管理员	• 正常	锁定:重置密码
	staff01	王小明		-	-	● 锁定	激活 重置密码 权限分配

图 3-4 查看用户数

3. 激活租户用户并授予角色

(1)登录实验平台对应实验拓扑左侧的管理机,进入管理机,打开浏览器,在地址栏 中输入云安全平台的 IP 地址"https://10.95.134.52"(以实际设备 IP 地址为准),进入云 安全平台的登录界面。输入安全管理员用户名密码 secadmin/csmp@qihoo360(以实际 用户名/密码为准),单击"立即登录"按钮进入云安全平台。

(2)单击"用户管理"→"租户"按钮,进入租户列表,单击"技术部"条目右侧的"查看 详情"按钮。

(3) 在"技术部"的用户列表中,单击 staff01 用户右侧的"激活"按钮,如图 3-5 所示。

用户管机	理 / 租户 / 技术部 操编作 × 词 输入账号搜索	Q					
	用户账号	姓名	邮箱	手机	角色	状态	操作
	TechDepartment_aud	租户审计管理员	-	-	租户审计管理员	• 正常	锁定 = 重置密码
	TechDepartment_sec	租户安全管理员	-	-	租户安全管理员	• 正常	锁定 重置密码
	TechDepartment_sys	租户系统管理员	-	-	租户系统管理员	• 正常	锁定 = 重置密码
	staff01	王小明		-	租户系统管理员	• 正常	锁定 : 重置密码 : 权限分配
						共4条	10条 v (1 >

图 3-5 用户列表界面

(4) 确认激活用户,单击"确定"按钮。

(5) 激活成功,可以看到 staff01 用户的"状态"由"锁定"转变为"正常"。

(6) 单击 staff01 用户列表右侧的"权限分配"按钮。

(7) 单击"选择角色类型"下拉菜单中的"租户系统管理员"选项,单击"保存"按钮。

(8)返回"技术部"的租户界面,可以看到"账号"为 staff01 的用户角色分配成功。激活此账号并赋予权限后可使用此账号登录云安全管理平台,如图 3-6 所示。

系統管理 / 订单审核流程 +新端 批量操作 >	设置 请输入租户名搜索	Q		
流程名称	流程策略	审核流程	关联租户	操作
默认流程	手动审核	一级审核人员:系统管理员	技术部	编辑 切换自动审核
				共1条 10条 > < 1

图 3-6 角色分配成功

4. 设置订单审核方式

(1)登录实验平台对应实验拓扑左侧的管理机,进入管理机,打开浏览器,在地址栏 中输入云安全平台的 IP 地址"https://10.95.134.52"(以实际设备 IP 地址为准),进入云 安全平台的登录界面。输入系统管理员用户名密码 sysadmin/csmp@qihoo360(以实际 用户名/密码为准),单击"立即登录"按钮,进入云安全平台。

(2)单击界面左侧"系统管理"按钮→单击"订单审核流程设置"按钮,在此界面设置 订单审核流程以及审核方式。此界面中包括一条默认流程,并自动关联平台中的所有租 户,单击界面右侧"编辑"按钮。

(3)设置"流程策略"为"手动审核","一级审核人员"为"系统管理员",配置结束,单击"保存"按钮。

(4) 订单审核流程配置成功,如图 3-7 所示。

系统管理 / 订单审核流程设 + 新增 批量操作 >	置 请输入租户名搜索	Q		
流程名称	流程策略	审核流程	关联租户	操作
默认流程	手动审核	一级审核人员:系统管理员	技术部	编辑 切换自动审核
				共1条 10条 > < 1

图 3-7 配置成功

5. 申请安全组件

(1)登录实验平台对应实验拓扑左侧的管理机,进入管理机,打开浏览器,在地址栏 中输入云安全平台的 IP 地址"https://10.95.134.52"(以实际设备 IP 地址为准),进入云 安全平台的登录界面。输入租户用户的用户名/密码为 staff01/xiaoming(以实际注册的 用户名/密码为准),单击"立即登录"按钮,进入云安全平台。

(2) 登录云安全平台后,显示云安全平台的面板界面。

(3) 单击界面左侧"安全组件"按钮→单击"我的组件"按钮,可以看到该租户下没有

安全组件。

(4)单击界面左侧"安全组件"按钮→单击"安全资源池"按钮。单击虚拟化安全管理系统中的"立即开通"按钮。

(5)选择"网络分区"为 vlan_subnet,输入"设备名称"为 TechDepartment01(由于并 行操作人员可能较多,为避免命名冲突,建议使用学生个人名字进行命名),选择"Linux 终端数"为 10,其他保留默认配置,单击"提交"按钮。

(6) 核实相关信息是否正确,确认无误后单击"完成"按钮。

(7)单击界面左侧"订单管理"按钮→单击"订单列表"按钮,在订单列表中,可以看到 此申请订单的"状态"为"审核中",如图 3-8 所示。

理 / 订单列表									
∨ 请输入搜	素条件	Q							안 导出
号 租户名称	账号 安全	组件类型 详情		状态	创建时间	审核时间	执行结果	操作	
技术部	staff01 虚拟	J化安全 购买,标准版	Linux终端数: 10, 1 个月	审核中	2018-06-07 16:27:55		-	查看 I	取消订单
						共1条 10条	v < 1		跳至 1
	5理 / 订单列表 → 清絶入授 号 租户名称 技术部	3理 / (1年列表 → 清添入微学条件 号 相户名称 账号 安全 技术部 staff01 虚形	3理 / 订単列表 √ 法部入股支条件 Q 号 租户名称 账号 安全組件类型 洋橋 技术部 staff01 虚拟化安全 购天 标准版.	3理 / 订单列表 > 法能入理安条件 Q 号 租户名称 账号 安全组件类型 详情 技术部 staff01 虚拟化安全 购买,标准版, Linux终跳数: 10, 1 个月 []	3理 / JJ単列表 √ 法総入理支条件 Q 号 租户名称 账号 安全組件类型 详情 状态 技术部 staff01 虚拟化安全 购买,标准纸, Linux终端数: 10, 1 个月 軍統中	1 J型手列表 ● 福户名称 账号 安全組件类型 洋倩 技术部 staff01 成形化安全 购死、标准版、Linux线跳散: 10, 1 个月 筆板中 2018-06-07 16:27:55	12理 / JT単列表 ◆ 法部入股资金件 Q 号 租户名称 账号 安全指件类型 洋樽 状态 创建时间 単核时间 技术部 staff01 虚积化安全 购买 标准版、Linux终跳数: 10. 1 个月 単核中 2018-06-07 16:27:55 - 共1 条 10 条。	12 / J1単列表 2 注意人意思条件 Q 号 租户名称 解号 安全組件英型 详情 次态 創建初同 単統対同 执行地果 技术部 staff01 虚拟化安全 购死,标准紙、Linux代读数: 10, 1 个月 単統中 2018-06-07 16:27:55 共1条 10 を…> < 1	12 / J1争列表 ▲ 本 2 3 4 10 10 10 10 10 10 10 10

图 3-8 等待审核

(8)登录实验平台对应实验拓扑左侧的管理机,进入管理机,打开浏览器,在地址栏 中输入云安全平台的 IP 地址"https://10.95.134.52"(以实际设备 IP 地址为准),进入云 安全平台的登录界面。输入系统管理员用户名密码"sysadmin/csmp@qihoo360"(以实际 用户名/密码为准),单击"立即登录"按钮,进入云安全平台。

(9)单击界面左侧"订单管理"按钮→单击"订单审核"按钮,可以看到由 staff01 租户 用户提出的订单申请信息,单击右侧"审核"按钮,通过此申请。

(10) 选择"审核通过",单击"确认"按钮。

(11)返回"订单审核"界面,可以看到由 staff01 用户提出的订单申请"状态"为"审核 通过",如图 3-9 所示。

Γ	订单管理 /	订单审核						
	全部	➤ 请输入搜索	委任	Q				
	订单号	租户名称	账号	安全组件类型	详情	状态	创建时间	审核时间
	13	技术部	staff01	虚拟化安全	购买,标准版,Linux终端数:10,1 个月	● 审核通过	2018-06-07 16:27:55	2018-06-07 17:16:12

图 3-9 审核通过

(12)单击界面左侧"安全组件"按钮→单击"我的组件"按钮,在组件列表中,可以看 到"组件名称"为 TechDepartment01 的安全组件"状态"由"创建中"转变为"初始化中", 如图 3-10 所示。

(13) 等待虚拟化安全组件创建及初始化结束,"状态"转变为"运行中",如图 3-11 所示。

6. 创建虚拟机

(1)登录实验平台对应实验拓扑左侧的管理机,进入管理机,打开浏览器,在地址栏 中输入安全云设备的域名"http://u.mcloud.cn"(以实际域名为准),进入安全云系统的

HH 概览		安全组	牛 / 我的组作	\$											
圆 安全组件	~	批量	操作 ~	全部	授	又不足2月(0) 所	有	▼ 清输.	∖搜索条件	Q					12 导出
我的组件			租户名称	账号	可用区域	组件名称		安全组件类型	规格	计量开始时间	计量结束时间	剩余授权数	IP	状态	操作
安全资源池			技术部	staff01	北京一区	TechDepartment	t01	虚拟化安全	标准版	-	-	0	10.95.141.10	* 初始化中	详情
🗟 订单管理	>										共	1 条 10 条/页	v < 1	> 跳至	1 页

图 3-10 创建安全组件

安全	全组件	/ 我的组修												
掛	t 量操	/fE ~	全部	₿	授权不足2月(1)	所有	 请输 	入搜索条件	Q					12 导出
		租户名称	账号	可用区域	组件名称	安全组件类型	规格	计量开始时间	计量结束时间	剩余授权数	IP	状态	操作	
C		技术部	staff0 1	北京一区	TechDepartment 01	虚拟化安全	标准 版	2018-06-07 17: 18	2018-07-07 00: 00	10	10.95.141. 10	•运行 中	访问:详情	■更多∨
										共1条 10	条/页 >	< 1	> 跳至	1 页

图 3-11 安全组件创建成功

登录界面。输入用户名/密码 admin/123456(以实际的注册账号/密码为准)登录安全云 系统。单击"登录"按钮。

(2) 登录安全云系统主界面,单击界面左侧功能栏中的"计算"按钮。

(3)进入"计算"模块下面的"虚拟机管理"界面。在"虚拟机管理"界面中,单击界面 右侧"创建虚拟机"按钮。

(4) 进入"虚拟机配置"界面,可根据不同需求创建不同种类的虚拟机。

(5) 在"虚拟机配置"界面中,单击"选择集群"下拉菜单中的 nova 选项,单击"选择镜像"下拉菜单中的 CentOS-7.2-64bit 选项,集群和镜像为必选项。选择网络为 vlan。

(6) 在"虚拟机配置"界面下方,选择"子网名称"为 vlan_subnet。单击"下一步" 按钮。

(7)继续进行虚拟机配置,填写"虚拟机名称"为 TechDepartment,填写"登录账号" 名称为 Admin,填写此账号的"登录密码"为 Admin1234。配置结束,单击"完成"按钮。

(8)等待虚拟机创建成功,在界面右侧的虚拟机列表中,可以看到"虚拟机名称"为 TechDepartment的虚拟机的"状态"为"运行中","IP 地址"为 10.95.141.14。

(9)选择"虚拟机名称"为 TechDepartment 的虚拟机,单击"操作"中的"更多"按钮, 单击"连接终端"命令进入虚拟机,如图 3-12 所示。

(10) 连接终端成功。输入"login/Password"为"Admin/Admin1234",即可成功登录 虚拟机,如图 3-13 所示。

7. 下载安装虚拟化客户端

(1) 在命令行输入下载命令"wgethttps://10.95.141.6:8443/download/360linuxc
(10.95.141.6_8080_8090).sh--no-check-certificate"从虚拟化安全平台中下载虚拟化安全
管理系统 Linux 客户端安装包(以实际下载地址为准)。输入命令后,按 Enter 键,等待下载结束,如图 3-14 所示。

(2) 输入安装命令"sudo bash 360linuxc\(10.95.141.6_8080_8090\).sh",按 Enter

计算 > 虚拟机管理											
IP或IP段 ▼ 请输入II	?或IP段模糊	查询	搜索	重置	高级搜索						口创建虚拟标
□ 虚拟机名称 所属集	鮮 监控	IP地址	状态	网络类型	镜像名称	高可用	业务组个数	创建时间	÷	用户名称	操作
🔲 TechDepartment 🕅 Dva	4	(内) 10.95.141.14	⊗运行中	vlan网络	Cent0S-7.2-64bit	关闭	0	2018-06-0	1 16:41:16	admin 番白	查看更多
启动 关机 删除	重启	关机迁移	在线迁移			每页显示	10 条 第	1页/共:	ц трк	- 単内 - 关机 - 注接後	2.##
										開除虚	ing a拟机
										关联福	份策略

图 3-12 连接终端

Connected (unencrypted) to: QEBU (instance-00000064)
CentOS Linux 7 (Core) Kernel 3.10.0-327.el7.x86_64 on an x86_64
techdepartment login: Admin Password: Last login: Thu Jun ? 10:37:07 on tty1 [Admin@techdepartment ~]\$

图 3-13 成功登录虚拟机



图 3-14 下载安装包

键,输入 Admin 用户密码 Admin1234,再次按 Enter 键开始安装。在安装 Linux 终端时, 会让用户确认操作系统版本信息,若系统版本与用户的操作系统版本一致时,直接按 Enter 键即可,若版本不一致则需要选择对应的版本,再按 Enter 键。此处输入"2",按 Enter 键,如图 3-15 所示。

(3)等待安装结束,可以看到虚拟化安全管理系统 Linux 客户端安装包成功安装并运行,如图 3-16 所示。

【实验预期】

(1) 查看安装结果。

(2) 卸载虚拟化安全管理系统 Linux 客户端安装程序。

[Admin@techdepartment ~]\$ sudo bash 360linuxc\(10.95.141.6_8080_8090\).sh
LsudoJ password for Admin ter and a second second
ARREAL ARREAL ARREAL ARREAL AND A A A A A A A A A A A A A A A A A A
##Currently the following Linux systems could be supported:
1: ubuntu 10-14
2: centos 5-7
3: redhat 5-7
4: suse 11-12
Your current os-system is:centos 7.2.1511
Please straightly press 'Enter' key, you can download and install the linux clie
nt;
If your system type is incorrectly identified, you should enter the number in the
e table, then press 'Enter' key!

图 3-15 执行安装命令



图 3-16 成功安装并运行

【实验结果】

(1)返回管理机浏览器中的虚拟化安全管理系统界面,在组件列表中找到"虚拟化安 全"组件,单击"访问"按钮,如图 3-17 所示。

安约	全组件	/ 我的组	4											
Ħ	比量操	作 ~	全部	ß	授权不足2月(1)	所有	 请输 	入搜索条件	Q					12 导出
		租户名称	账号	可用区域	组件名称	安全组件类型	规格	计量开始时间	计量结束时间	剩余授权数	IP	状态	操作	
(技术部	staff0 1	北京一区	TechDepartment 01	虚拟化安全	标准 版	2018-06-08 10: 14	2018-07-08 00: 00	9	10.95.141. 11	•运行 中	访问	洋情∣更多 ∨
										共1条 10)条/页∨	< 1	> 8	1页

图 3-17 "虚拟化安全"组件

(2) 单击左侧"主机管理"按钮下的"病毒查杀"按钮,可以看到 TechDepartment 主机 已在线,如图 3-18 所示。

(3) 返回 Linux 客户端,输入命令"cd /opt/360safe"进入安装目录,如图 3-19 所示。

(4) 输入卸载命令"sudo sh uninstall.sh",按 Enter 键,输入 Admin 用户密码 Admin1234,再次按 Enter 键。等待卸载结束即完成了虚拟化安全管理系统 Linux 客户 端的卸载,如图 3-20 所示。

品 概読	主机分组	6	主机管理 > 病毒查杀 > 全(司主机			
目主机管理	 全网主机 默认分组 					□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□	关键字
病毒查杀			□ 主机名称	IP	揭作系统	(病毒/太马	F次扫描时间
webshell扫描					0007	//344///4-5	
安全基线			techdepartment	10.95.141.14	CentOS /		
防暴力破解			TechDp	10.95.141.13	Windows Server 2008 R2 SP 1		
虚拟化加固			快速扫描 全盘扫描	强力查杀 隔离区恢复	全部操作 💌	毎页显示 10 条 第 1 页 / 共 1 页	к с 1
网卡流量统计		-					
升级管理							
资产管理 >							
論 防火墙							
▲ 入侵防御							

图 3-18 主机列表



图 3-19 进入安装目录

【实验思考】

(1) 关机状态下,在"主机管理"界面中,主机的状态应是什么?

(2) 卸载虚拟化安全管理系统后,在"主机管理"界面中,主机的状态应是什么?

3.1.2 虚拟化安全管理系统 Windows 客户端安装及卸载实验

【实验目的】

安装虚拟化安全客户端。

【知识点】

虚拟化安全管理、Windows 客户端安装卸载。

【场景描述】

A 公司虚拟化安全管理系统控制中心服务器部署完毕后,需要在虚拟化安全管理系统管理的主机中安装客户端程序。主机分为两种操作系统:Windows和Linux。安全运维工程师小王需要为所辖Windows主机配置虚拟化安全管理系统客户端,熟悉客户端的安装、卸载流程,请帮助小王熟悉虚拟化安全管理系统Windows客户端的配置。

【实验原理】

管理员可通过云安全管理平台中的"安全组件"模块,找到虚拟化安全组件,访问虚拟 化安全组件后,可以下载安装虚拟化客户端。

【实验设备】

安全设备:云安全设备1台。

图 3-20 卸载成功

基础设施:安全云设备1台。 主机终端:Windows7主机1台。

【实验拓扑】

实验拓扑如图 3-21 所示。



图 3-21 虚拟化安全管理系统 Windows 客户端安装及卸载实验拓扑图

【实验思路】

- (1) 登录云安全管理平台。
- (2) 创建租户以及租户用户。
- (3) 租户用户申请安全组件。
- (4) 登录安全云平台,创建虚拟机。
- (5) 下载安装虚拟化客户端。
- (6) 卸载客户端。

【实验步骤】

1. 登录云安全平台

(1)登录实验平台对应实验拓扑左侧的管理机,进入管理机,打开浏览器,在地址栏 中输入云安全平台的 IP 地址"https://10.95.134.52"(以实际设备 IP 地址为准),进入云 安全平台的登录界面。输入系统管理员用户名密码"sysadmin/csmp@qihoo360"(以实际 用户名/密码为准),单击"立即登录"按钮,进入云安全平台。

(2) 登录云安全平台后,显示云安全平台的面板界面。

2. 新建租户以及租户用户

(1) 单击左侧"用户管理"按钮→单击"租户"按钮,进入租户管理界面。

(2) 在"租户"界面中,单击"+添加租户"按钮,添加一个租户。

(3) 在弹出的"添加租户"对话框中,填写"租户 ID"为 TechDepartment(由于并行操 作人员可能较多,为避免命名冲突,建议使用学生个人名字进行命名),填写"租户名称"为"技术部",填写"描述"为"技术部",单击"保存"按钮,新建技术部租户。

(4) 返回"租户"界面,可以看到新建技术部租户成功。

(5) 单击"租户"名称为"技术部"列表右侧的"查看详情"按钮,查看该租户的详细 信息。

(6) 进入"技术部"租户界面,单击"+添加租户用户"按钮,为该租户添加一个用户。

(7) 在弹出的"添加租户用户"界面中,填写"账号"为 staff01,填写"姓名"为"王小明" (由于并行操作人员可能较多,为避免命名冲突,建议使用学生个人名字进行命名),填写 "密码"为 xiaoming,填写"确认密码"为 xiaoming,填写"邮箱"为"xiaoming@360.net",填 写"描述"为"技术部员工",单击"保存"按钮。

(8) 返回"技术部"租户界面,可以看到已成功新建租户用户,如图 3-22 所示。

用户管	理 / 租户 / 技术部	请编入账号搜索 Q					
	用户账号	姓名	邮箱	手机	角色	状态	操作
	TechDepartment_aud	租户审计管理员	-	-	租户审计管理员	• 正常	编辑
	TechDepartment_sec	租户安全管理员	-	-	租户安全管理员	• 正常	编辑
	TechDepartment_sys	租户系统管理员	-	-	租户系统管理员	• 正常	编辑
	staff01	王小明		-	-	• 锁定	编辑:删除
	L				共4条	10 条 > (1	> 跳至

图 3-22 新建租户用户成功

(9) 单击界面上方"租户"按钮,返回"租户"界面,可以看到"技术部"租户下的"用户数"变为4,成功新建用户,如图 3-23 所示。

用户1	智理/ 租户 参加租户 批量删除	请输入租户名称搜索 Q]			
	租户名称	租户ID	描述	创建时间	用户数	操作
	技术部	TechDepartment	技术部	2018-06-07 14:30:35	4	查看详情:编辑:删除
					共1条	10 条 > (1

图 3-23 查看用户数

3. 激活租户用户并授予角色

(1)登录实验平台对应实验拓扑左侧的管理机,进入管理机,打开浏览器,在地址栏 中输入云安全平台的 IP 地址"https://10.95.134.52"(以实际设备 IP 地址为准),进入云 安全平台的登录界面。输入安全管理员用户名密码"secadmin/csmp@qihoo360"(以实际 用户名/密码为准),单击"立即登录"按钮进入云安全平台。 (2)单击"用户管理"按钮→单击"租户"按钮,进入租户列表,单击"技术部"条目右侧的"查看详情"按钮。

(3) 在"技术部"的用户列表中,单击 staff01 用户右侧的"激活"按钮,如图 3-24 所示。

用户管	理/租户/技术部						
批	≧操作 ∨ ☐ 请输入账号搜索	Q					
	用户账号	姓名	邮箱	手机	角色	状态	操作
	TechDepartment_aud	租户审计管理员	-	-	租户审计管理员	• 正常	锁定:重置密码
	TechDepartment_sec	租户安全管理员	-	-	租户安全管理员	• 正常	锁定:重置密码
	TechDepartment_sys	租户系统管理员	-	-	租户系统管理员	• 正常	锁定:重置密码
	staff01	王小明		-		• 锁定	激活重置密码 权限分配

图 3-24 用户列表界面

(4) 确认激活用户,单击"确定"按钮。

(5) 激活成功,可以看到 staff01 用户的"状态"由"锁定"转变为"正常"。

(6) 单击 staff01 用户列表右侧的"权限分配"按钮。

(7) 单击"选择角色类型"下拉菜单中的"租户系统管理员"选项,单击"保存"按钮。

(8)返回"技术部"的租户界面,可以看到"账号"为 staff01 的用户角色分配成功。激活此账号并赋予权限后即可使用此账号登录云安全管理平台,如图 3-25 所示。

用户管	理/租户/技术部						
批量	└撮作 ∨ 」 请输入账号搜索	Q					
	用户账号	姓名	邮箱	手机	角色	状态	操作
	TechDepartment_aud	租户审计管理员	-	-	租户审计管理员	• 正常	锁定□重置密码
	TechDepartment_sec	租户安全管理员	-	-	租户安全管理员	• 正常	锁定 重置密码
	TechDepartment_sys	租户系统管理员	-	-	租户系统管理员	• 正常	锁定・重置密码
	staff01	王小明		-	租户系统管理员	• 正常	锁定:重置密码:权限分配
						共4条 1	0ዷ ∨ < 1 >

图 3-25 角色分配成功

4. 设置订单审核方式

(1)登录实验平台对应实验拓扑左侧的管理机,进入管理机,打开浏览器,在地址栏 中输入云安全平台的 IP 地址"https://10.95.134.52"(以实际设备 IP 地址为准),进入云 安全平台的登录界面。输入系统管理员用户名密码"sysadmin/csmp@qihoo360"(以实际 用户名/密码为准),单击"立即登录"按钮,进入云安全平台。

(2)单击界面左侧"系统管理"按钮→单击"订单审核流程设置"按钮,在此界面设置 订单审核流程以及审核方式。此界面中包括一条默认流程,并自动关联平台中的所有租 户,单击界面右侧"编辑"按钮,如图 3-26 所示。

(3)设置"流程策略"为"手动审核","一级审核人员"为"系统管理员",配置结束,单击"保存"按钮。

(4) 订单审核流程配置成功。

🗄 概覧		系统管理 / 订单审核流程	设置			
☑ 安全组件	>	+ 新増 批量操作 ∨	请输入租户名搜索	Q		
🗟 订单管理	>	流程名称	流程策略	审核流程	关联租户	操作
: 费用管理	>	默认流程	手动审核	一级审核人员:系统管理员	技术部	编辑 如换自动审核
А。用户管理	>					共1条 10条 > < 1
③ 系统管理	~					
授权管理						
订单审核流	程设置					
通知设置						
引流设置						
系统对接						

图 3-26 设置订单审核方式

5. 申请安全组件

(1)登录实验平台对应实验拓扑左侧的管理机,进入管理机,打开浏览器,在地址栏 中输入云安全平台的 IP 地址"https://10.95.134.52"(以实际设备 IP 地址为准),进入云 安全平台的登录界面。输入租户用户的用户名/密码为"staff01/xiaoming"(以实际注册 的用户名/密码为准),单击"立即登录"按钮,进入云安全平台。

(2) 登录云安全平台后,显示云安全平台的面板界面。

(3)单击界面左侧"安全组件"按钮→单击"我的组件"按钮,可以看到该租户下没有 安全组件。

(4)单击界面左侧"安全组件"按钮→单击"安全资源池"按钮。单击虚拟化安全管理 系统中的"立即开通"按钮。

(5)选择"网络分区"为 vlan_subnet,输入"设备名称"为 TechDepartment01(由于并 行操作人员可能较多,为避免命名冲突,建议使用学生个人名字进行命名),选择"Linux 终端数"为 10,其他保留默认配置,单击"提交"按钮。

(6) 核实相关信息是否正确,确认无误后单击"完成"按钮。

(7)单击界面左侧"订单管理"按钮→单击"订单列表"按钮,在订单列表中,可以看到 此申请订单的"状态"为"审核中",如图 3-27 所示。

Β	8 概覧		订单	単管理 /	订单列表										
B	3 安全组件		全	部	▼ 清輸入計	夏索条件	Q								2 导出
ē	3 订单管理	~	ប	伸号	租户名称	账号	安全组件类型	详情		状态	创建时间	审核时间	执行结果	操作	
	订单列表	:	13	3	技术部	staff01	虚拟化安全	购买,标准版,	Linux终端数: 10, 1 个月	审核中	2018-06-07 16:27:55	-		查看	取消订单
	订单审核											共1条 10条			跳至 1
E	日志管理														
0	3 费用管理														
1	。 用户管理														
6) 系统管理														

图 3-27 等待审核

(8) 登录实验平台对应实验拓扑左侧的管理机,进入管理机,打开浏览器,在地址栏

中输入云安全平台的 IP 地址"https://10.95.134.52"(以实际设备 IP 地址为准),进入云 安全平台的登录界面。输入系统管理员用户名密码 sysadmin/csmp@qihoo360(以实际 用户名/密码为准),单击"立即登录"按钮,进入云安全平台。

(9)单击界面左侧"订单管理"按钮→单击"订单审核"按钮,可以看到 staff01 租户用 户提出的订单申请信息,单击右侧"审核"按钮,通过此申请,如图 3-28 所示。



图 3-28 单击"审核"

(10) 选择"审核通过",单击"确认"按钮。

(11)返回"订单审核"界面,可以看到由 staff01 用户提出的订单申请"状态"为"审核 通过",如图 3-29 所示。

订单	管理 /	订单审核						
全部	ıß	∨ 请输入搜索	素条件	Q				
订	单号	租户名称	账号	安全组件类型	详情	状态	创建时间	审核时间
13		技术部	staff01	虚拟化安全	购买,标准版,Linux终端数:10,1 个月	● 审核通过	2018-06-07 16:27:55	2018-06-07 17:16:12

图 3-29 审核通过

(12)单击界面左侧"安全组件"按钮→单击"我的组件"按钮,在组件列表中,可以看 到"组件名称"为 TechDepartment01 的安全组件"状态"由"创建中"转变为"初始化中", 如图 3-30 所示。

88	概览		安全组	件 / 我的组织											
52	安全组件	~	批量	操作 >	全部	授	权不足2月(0) 所有	▼ 清输	入搜索条件	Q					1997年1月1日
[我的组件			租户名称	账号	可用区域	组件名称	安全组件类型	规格	计量开始时间	计量结束时间	剩余授权数	IP	状态	操作
	安全资源池			技术部	staff01	北京一区	TechDepartment01	虚拟化安全	标准版	-	-	0	10.95.141.10	*初始化中	详情
5	订单管理	>									共 1	条 10条/页	v < 1	> 跳至	1 页
ŧ	费用管理	>													
R	用户管理	>													
٢	系统管理	>													

图 3-30 创建安全组件

(13)等待虚拟化安全组件创建及初始化结束,"状态"转变为"运行中",如图 3-31 所示。

安全组体	= / 我的组	件											
批量換	¥fE ∨	全部	\$	授权不足2月(1)	所有、、	~ 请输	入搜索条件	Q					1993年1月11日
	租户名称	账号	可用区域	组件名称	安全组件类型	规格	计量开始时间	计量结束时间	剩余授权数	IP	状态	操作	
	技术部	staff0 1	北京一区	TechDepartment 01	虚拟化安全	标准 版	2018-06-07 17: 18	2018-07-07 00: 00	10	10.95.141. 10	•运行 中	访问:详	情↓更多 ∨
									共1条 10	条/页 >	< 1	> 跳至	图 1 页

图 3-31 安全组件创建成功

6. 创建虚拟机

(1)登录实验平台对应实验拓扑左侧的管理机,进入管理机,打开浏览器,在地址栏 中输入安全云设备的域名"http://u.mcloud.cn"(以实际域名为准),进入安全云系统的 登录界面。输入用户名/密码"admin/123456"(以实际的注册账号/密码为准)登录安全 云系统。单击"登录"按钮。

(2) 登录安全云系统主界面,单击界面左侧功能栏中的"计算"按钮。

(3)进入"计算"模块下面的"虚拟机管理"界面。在"虚拟机管理"界面中,单击界面 右侧"创建虚拟机"按钮,如图 3-32 所示。

计算	计算》 虚拟你管理
虚拟机管理	IT或IT投 * 济输入IT或IT投模糊宣词 被索 筆置 高级继索
· 鏡像管理	自 建拟机名称 所属集群 监控 IP地址 状态 网络类型 積像名称 高可用 业务组个数 创建时间 = 用户名称 操作
 ● 备份管理 	■ hort01 🖉 nova 🔄 (内) 10.16.4.3 ⑥运行中 私有网络 CantOS-7.2-64bit 关闭 0 2018-06-07.09:43:40 admin 查香 単多
▶ 3単性伸缩	■ TechNepartment 🖉 nova 🕞 (内) 10.95.141.14 《运行中 vlac网络 CentOS-7.2-64bit 美闲 0 2018-06-01 16:41:16 edmin 查看 三更多
	自动 关机 翻译 重自 关机迁移 在线迁移 每页显示 ⑩ 条 第 1页 / 共 1页 K < ● > >

图 3-32 虚拟机管理

(4) 进入"虚拟机配置"界面,可根据不同需求创建不同种类的虚拟机。

(5) 在"虚拟机配置"界面中,单击"选择集群"下拉菜单中的 nova 选项,单击"选择镜像"下拉菜单中的 Windows_Server_2008_R2_x64 选项,集群和镜像为必选项。选择网络为 vlan。

(6) 在"虚拟机配置"界面下方,选择"子网名称"为 vlan_subnet。单击"下一步" 按钮。

(7)继续进行虚拟机配置,填写"虚拟机名称"为 TechD,填写"登录账号"名称为 "Admin",填写此账号的"登录密码"为 Admin1234。配置结束,单击"完成"按钮。

(8)等待虚拟机创建成功,在界面右侧的虚拟机列表中,可以看到"虚拟机名称"为 TechDp的虚拟机的"状态"为"运行中","IP地址"为10.95.141.13。

(9)选择"虚拟机名称"为 TechDp 的虚拟机,单击"操作"中的"更多"按钮,单击"连接终端"命令进入虚拟机,如图 3-33 所示。

(10) 单击界面右上角 Send CtrlAltDel 按钮,进入虚拟机,如图 3-34 所示。

(11) 单击 Admin 按钮,选择此账号进行登录。

云计算及云安全实验指导 💼

计算 > 虚拟机管理											
IP或IP段 · 〕	请输入IP或IP段	模糊	查询	搜索	重置高级推	安索					口创建虚拟机
□ 虚拟机名称	所属集群	站控	IP地址	状态	网络类型	镜像名称	高可用	业务组个数	创建时间 👳	用户名	称 操作
🗉 TechDp 🗹	nova	47	(内) 10.95.141.13	◎运行中	vlan网络	Windows_Server_2008_B2_x64	关闭	0	2018-06-08 15:34:31	admin	查看 更多
🔲 hostOl 🗹	nova	42	(内) 10.16.4.3	◎运行中	私有网络	CentOS=7.2=64bit	关闭	0	2018-06-07 09:43:40	admin	关机
TechDepartment	Znova	42	(内) 10.95.141.14	◎运行中	vlan网络	CentOS=7.2=64bit	关闭	0	2018-06-01 16:41:16	admin	连接终端 刪除虚拟机
启动 关机	删除 重)		关机迁移 在线过	ERB				每页显示 10]条 第 1 页 / 共 1 页	к	关联备份策略 从备份中恢复 关联业务组 创建造像
											升级配置

图 3-33 连接终端



图 3-34 进入虚拟机

(12) 输入密码为 Admin1234,按 Enter 键,即可成功登录虚拟机。

7. 下载安装虚拟化安全管理系统客户端

(1) 进入虚拟机,单击"开始"按钮,选择 IE 浏览器,如图 3-35 所示。

(2) 将云安全管理平台 IP 地址添加至可信站点,选择浏览器右上角"工具"→ "Internet 选项"菜单命令。

(3) 在"Internet 选项"对话框中选择"安全"选项卡,单击"受信任的站点"按钮,单击"站点"按钮,添加站点。

(4) 在"受信任的站点"对话框中输入云安全管理平台 IP 地址"https://10.95.134. 52/"(以实际 IP 地址为准),单击"添加"按钮,配置结束,单击"关闭"按钮。

(5) 单击"确定"按钮,结束配置。

(6) 在地址栏中输入云安全管理平台的 IP 地址"https://10.95.134.52"(以实际设备 IP 地址为准),出现安全提示界面,在"安全警告"对话库中勾选"以后不再显示该警告"复选框,单击"确定"按钮。

(7) 单击"继续浏览此网站"按钮。

(8) 进入云安全管理平台的登录界面。在 界面文本输入框中输入管理员用户名和密码 "sysadmin/csmp@qihoo360"(以实际用户名/ 密码为准),单击"立即登录"按钮,进入云安全 平台。

(9)登录云安全平台后,显示云安全平台的面板界面。

(10)在云安全平台的面板界面,单击左侧"安全组件"按钮→单击"我的组件"按钮,进入云安全管理平台"我的组件"界面。

(11) 找到"虚拟化安全"组件,单击右侧 "访问"按钮。

(12)可以看到虚拟化安全的站点地址为"https://10.95.141.11:8443"(以实际页面显示 IP地址为准)。将虚拟化安全地址添加至可

 ○○○ 命令提示符 ○○○ ○○ ○○○ ○○○ ○○○ ○○○ ○○○ ○○○ ○○○ ○○○ ○○○ ○○ ○○	3
E Internet Explorer	Admin
PU	文档
	计算机
	网络
	控制面板
	设备和打印机
	管理工具 ▶
	帮助和支持
	运行
▶ 所有程序	
搜索程序和文件	注销 ▶
1772 🛃 🛃 📑	

图 3-35 选择 IE 浏览器

信站点,选择浏览器右上角"工具"→"Internet 选项"菜单命令。

(13) 在"Internet 选项"对话框中选择"安全"选项卡,单击"受信任的站点"按钮,单击 "站点"按钮,添加站点,如图 3-36 所示。

(14)在"受信任的站点"对话框中输入"https://10.95.141.11:8443/"虚拟化安全 IP
 地址(以实际虚拟化安全 IP 地址为准),单击"添加"按钮,配置结束,单击"关闭"按钮,如
 图 3-37 所示。

Internet 选项				? ×					
常规安全	隐私 内部	容 连接	程序 高級						
选择一个区域	以查看或更改步	全设							
	ľ,	\checkmark	0	^					
Internet	本地 Intranet	受信任的站	受限制的站	-					
	受信任的站点 该区域包含你确信不会损害你的计算机或文 住的对站。								
该区域的安全	【中有网站。 ≧级别 (L) ── □许级别:全部								
	- - 中 - 下载地在不安全内容前提示 不下载未签裡的 Activež 控件 								
□ 启用保排 启动 In	補式 (要求重新 ternet	新 自定义级务	(C) 默认	(銀別(O))					
		将所有区	区域重置为默认	级别(B)					
		确定	取消	应用(A)					

图 3-36 添加站点

(15) 单击"确定"按钮,结束配置。

(16)返回"我的组件"界面,找到"虚拟化 安全"组件,单击右侧"访问"按钮。

(17) 在打开的"虚拟化安全"页面,单击"主机管理"按钮→单击"资产管理"按钮→单击"虚拟化管理"按钮。

(18) 单击"安装包下载"按钮。

(19) 在弹出的"安装包下载"对话框中,选择"Windows 安装包",单击右侧"下载"按钮。

(20) 在弹出的下载确认对话框中,单击 "保存"按钮。

(21)等待下载结束,在虚拟机中进入下载 存储目录,找到文件安装包(若下载状态为安 全检查,则忽略,进入下载目录即可)。

(22)双击安装包,弹出权限认证对话框, 单击"是"按钮。

- (23) 在安装界面单击"立即安装"按钮,等待安装结束。
- (24) 安装结束,单击"完成"按钮。

【实验预期】

- (1) 查看到虚拟化客户端已经安装成功。
- (2) 卸载客户端成功。

【实验结果】

(1) 在管理机中查看已经安装成功的虚拟化客户端,如图 3-38 所示。

受信任的站点 圣 问以添加和删除该区域的网站。该区域中的所有网站都使 用区域的安全设置。	
将该网站添加到区域 0): [https://10.95.141.11:8443/] 阿站 (?): https://10.95.134.52 https://oca.microsoft.com https://ugate.microsoft.com	回收站
「 对该区域中的所有站点要求服务器验证 (https:)(5) 关闭(C)	260虚拟化

图 3-37 输入 IP 地址

图 3-38 安装成功

(2)返回管理机浏览器中的虚拟化安全管理系统界面,在组件列表中找到"虚拟化安全"组件,单击"访问"按钮,如图 3-39 所示。

安全	组件	/ 我的组修	4											
批	量操	۴×	全部	ß	授权不足2月(1)	所有	 请输 	入搜索条件	Q					12 号出
		租户名称	账号	可用区域	组件名称	安全组件类型	规格	计量开始时间	计量结束时间	剩余授权数	IP	状态	操作	
		技术部	staff0 1	北京一区	TechDepartment 01	虚拟化安全	标准 版	2018-06-08 10: 14	2018-07-08 00: 00	9	10.95.141. • 11	运行中	访问 详	情⊤更多 ∨
										共1) 象/页 ∨ <	1	> \$K3	至 1 页

图 3-39 "虚拟化安全"组件

(3) 单击左侧"主机管理"下的"病毒查杀"按钮,可以看到 TechDp 主机已在线,如 图 3-40 所示。

(4) 单击左下角"开始"按钮,单击"控制面板"按钮,如图 3-41 所示。

(5) 单击"卸载程序"按钮,如图 3-42 所示。

(6) 右击"虚拟化"按钮,选择"卸载/更改"。

(7) 在卸载窗口单击"卸载"按钮。

88 概选	主机分组		主机管理 > 病毒	查杀 > 全网主机			
書 主机管理 ✓	■ 全网主机 默认分组						筛选 ♥ 请输入关键
病毒查杀			□ 主机名称	IP	操作系统		病毒/木马 」
webshell扫描 ホムオゲ			TechDp	10.95.141.13	Windows Server 2008 F	12 SP 1	
安主圣成防暴力破解		(II	快速扫描	全盘扫描 强力查杀	隔离区恢复 全部操作 ▼	每页显示	10 条 第1页/共1页 14

图 3-40 主机列表

② Internet Explorer >	
 ↓ 记事本 ▲ 虚拟化 	Admin 文档
	计算机 网络
	控制面板 设备和打印更改您的计算机
	管理工具 > 和助和支持
▶ 所有程序	运行
被索程序和文件 2 0开始 1	

图 3-41 控制面板



图 3-42 卸载程序