天翼云终端防病毒产品
用户使用指南

中国电信股份有限公司云计算分公司

目录

1. 产品介绍

1.1 产品定义

随着虚拟化及云计算的发展，企业环境逐步由物理环境转变为由物理环境、私有云及公有云混合的环境，传统内外网的网络边界消失了；特别是在提供多租户服务的公有云中，不同组织的网络数据在数据中心内部、甚至是在同一台物理主机上进行交换，传统的安全设备已经无法对其进行检测及防护。云计算环境下需要基于每个终端节点、并且每个节点具有相同安全防护等级的全新的安全防护模型。

“终端杀毒”（以下又称“本服务”）以大数据技术为支撑、以可靠服务为保障，能够精确检测已知病毒木马、未知恶意代码，有效防御 APT 攻击，为企事业单位提供终端病毒、漏洞管控能力。

1.2 产品功能

1.2.1 恶意软件防护

支持对系统进行实时防护，定期对虚拟机进行全盘扫描，手动对虚拟机进行磁盘扫描。手动扫描支持快速、全盘、及指定目录扫描三种安全检测方式。感染的文件在虚拟机内部隔离。非虚拟机的用户，无权限读取隔离文件，避免数据泄露问题。优化安全操作的资源调度，以避免全系统扫描时出现常见的防病毒风暴。恶意代码特征库的自动更新，防范最新的攻击。

1.2.2 漏洞管理

- 提供对 Windows，Linux 部署系统安全风险的全面洞察，帮助快速和准确地识别、调查、划分优先级和纠正漏洞。
- 提供关于不断变化的 IT 环境中的所有资产和漏洞的最准确信息，帮助安全团队最大化效率和提高生产力。

- 支持 IPS 与漏洞扫描结果联动，在未安装实体补丁情况下，提供已知漏洞风险的安全防护。

1.2.3 实时扫描

通过强大的 QVM 引擎进行文件安全性的实时分析，并返回杀毒控制中心文件结果。

1.2.4 全盘扫描

包含快速扫描项目外的在内的，所有磁盘（当前所有挂载的）目录的文件；

1.2.5 强力查杀

自定义查杀强度，自定义方式对终端进行扫描，支持选择启用的引擎类型，配置是否自动处理，是否扫描信任区。

1.2.6 终端恢复

对终端隔离区指定时间段，指定文件路径或者文件名或者病毒文件进行恢复，恢复到原始路径。

1.2.7 隔离防护

隔离防护（下载文件存在风险性时进行沙箱运行防护）

1.2.8 定时查杀

对终端进行定时扫描，降低管理员的工作量。

1.2.9 云查杀

云查杀是终端启用防病毒云查。每次云查杀包括终端提交一批文件 MD5 到云查杀引擎，云查杀引擎鉴定完毕后给于反馈。

1.3 产品优势

1.3.1 防护新的云端威胁

- 防护在同一个数据中心、甚至是在同一主机上的两个虚拟机之间的攻击这种新的威胁，采用传统的网络安全设备无法检测。
- 病毒安全防护，可支持云桌面以及云主机多种场景下的病毒查杀功能，解决传统杀毒软件造成的启动、更新、查杀风暴问题。
- 自动检测虚拟机的系统和应用，并调整入侵检测的规则。使得虚拟机无需安装补丁即可防护利用系统漏洞的新的威胁。
- 未知威胁的防护，通过对海量访问日志数据的分析，找到异常行为、定位未知的安全威胁。

1.3.2 广泛的云平台的支持及统一管理

- 支持主流的虚拟化平台，包括 VMware、Xen、KVM 等。
- 与 OpenStack 的深度集成，支持绝大部分的国产云计算平台。
- 支持虚拟化平台部署和非虚拟化平台部署的统一安全管理。

1.3.3 更低运营成本

- 管理中心采用中央控管的管理方式，集中的配置每一台虚拟机的安全策略，提供了便捷的管理、更高的灵活性。
- 通过管理中心，可以为每个用户配置不同的安全策略。
- 安全特征库的自动升级，避免用户频繁升级系统补丁而引起的服务中断，降低了管理成本。

1.4 应用场景

针对企业用户或多个租户杀毒的场景，可采用控制中心版本，支持云主机和

云桌面环境的杀毒任务，用户可基于管理控制台，统一下发查杀任务，统一规划管控，查阅日志，统筹化管控防病毒任务。

支持由服务端发起病毒查杀任务，有效解决病毒的启动、查杀、更新造成的资源过度消耗风暴问题。

2. 操作指导

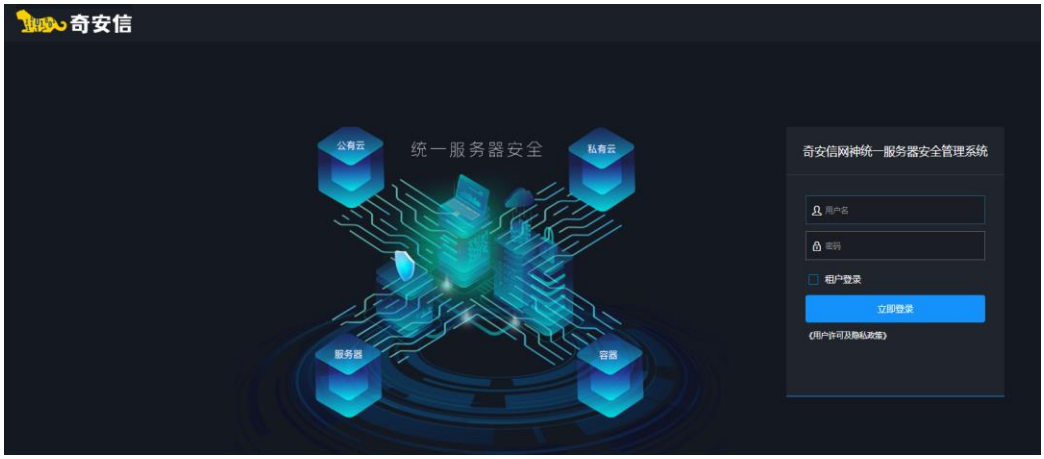
2.1 快速入门-控制中心版

2.1.1 安装控制中心

用户完成开通后，需自行在控制中心中开通云主机（使用终端杀毒镜像开通），并绑定弹性公网 IP。在控制中心中找到对应的终端杀毒实例获取 license。

2.1.2 登录

管理中心页面登录方式为 https://X.X.X.X:8447（X.X.X.X 就是第 1 步中为管理中心配置的 IP），其默认用户名密码为 **admin/sysadmin**，首次登录需要修改初始密码，管理员登录到系统后可进入 **管理->用户管理** 页面自己添加或删除用户。



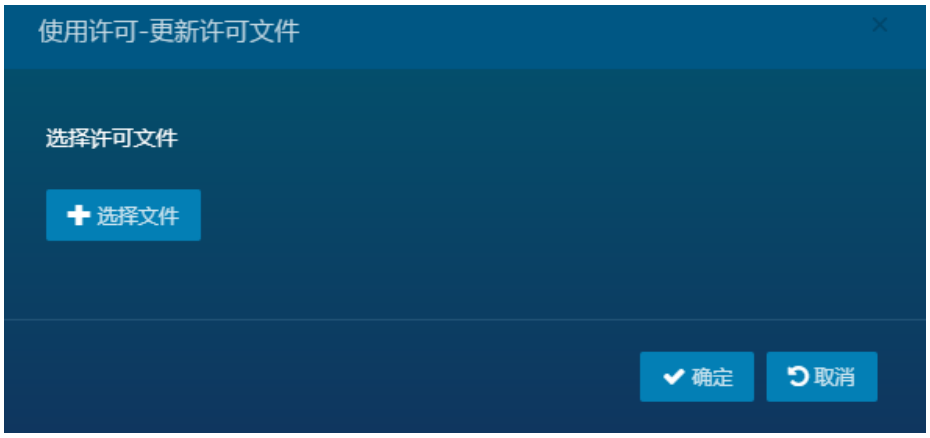
2.1.3 产品激活

初次进入管理中心时必须对产品进行激活才可以正常使用。

1)登录管理中心，进入**管理 ->系统设置->使用许可** 页面

2)在页面中点击 **更新许可文件** ，会打开如下图所示的 **使用许可 ->更新许**

可文件 对话框，选择正确的许可文件，点击 **确定**，即可激活。



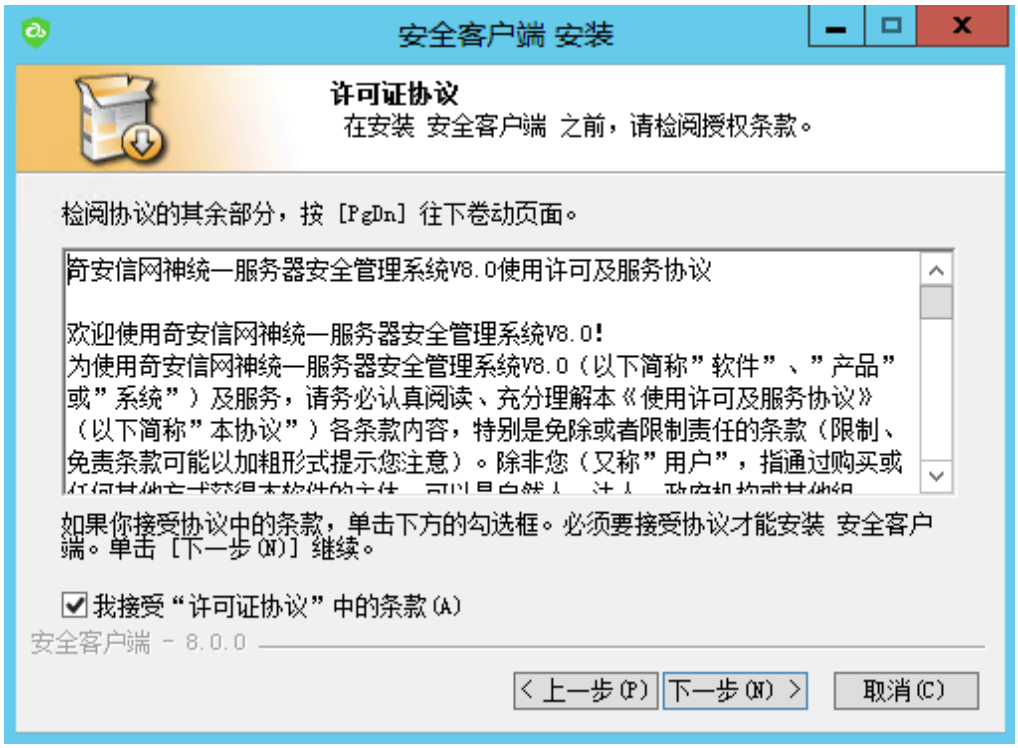
2.1.4 客户端安装

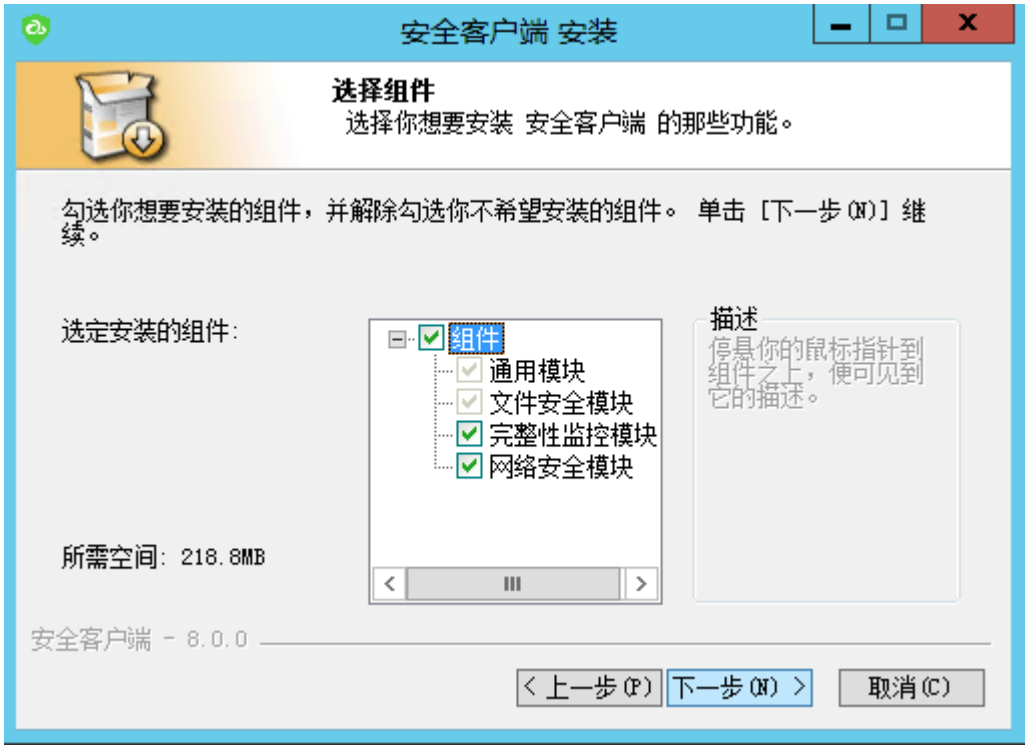
2.1.4.1 Windows 端

1. 在浏览器上通过访问 http://xxxx:8080/agent/ics-agent.exe，下载安装文件。

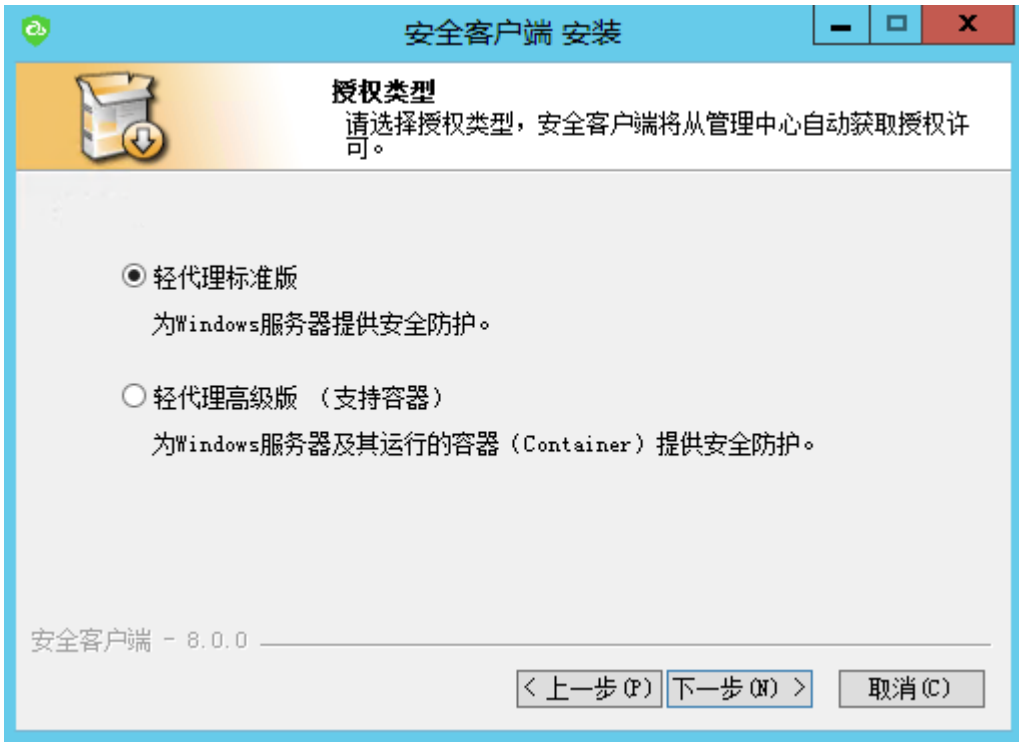
   （x.xx.x 是管理中心的 IP）

2. 执行安装文件，安装过程中可以选择是否安装网络模块和完整性监控模块。

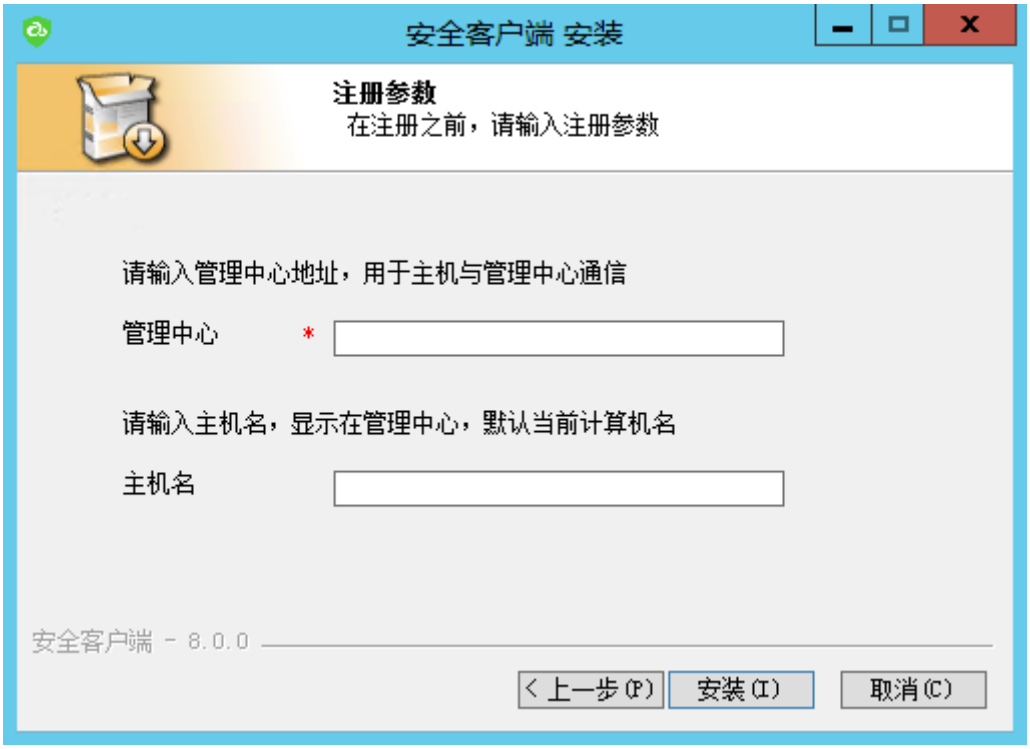




下一步之后根据需求选择轻代理标准版、轻代理高级版（支持容器）。



输入管理中心地址（必选）、主机名（可选），点击安装。



3. 注册成功后，管理中心能够看到该主机，主机状态显示为“已连接”，新注册的主机会被默认添加至名称为“新注册主机”的主机池中。

4. 管理中心 “资产管理”->“虚拟机/终端”页面能够看到该机器，其实时防护状态正确

2.1.4.2 Linux 端

方法 1：通过管理中心一键部署

1） 进入 **资产管理 ->主机** 页面

2） 在页面中点击 **新增** 按钮，会弹出 **新增主机池** 对话框，平台选择“非虚拟化平台”

3） 在对话框中输入主机池名称、选择添加方式、输入计算机名、IP 地址，点击确定即可。

参数说明：

名称 ：主机将要添加至的主机池名称，手动输入会新建一个以输入的名称命名的主机池、也可以选择管理中心现有的主机池。

添加方式：主机的添加方式分为单台计算机和网段范围内的多台计算机，默认为单台计算机，即一次添加一台主机；如果选择网段范围内的多台计算机，即一次性添加多台主机，如下图所示需要填写起始地址和结束地址。

计算机名：如果填写的是主机的域名，系统会根据域名去添加主机，不需要再输入计算

机 IP；如果填写的是主机的别名，则需要再输入正确的计算机 IP。

计算机 IP：主机的 IP 地址。

4） 添加成功后，主机状态为“未安装安全组件”

5） 选择刚才添加的主机，点击“安装安全组件”按钮

6） 在弹出的对话框中，输入主机用户名、密码（即 ssh 的用户名和密码），选择许可类型为服务器，点击确定，系统开始在主机上安装安全组件。

7） 安装安全组件过程中的状态变化由**未安装安全组件->正在安装->安装成功->连接中断->**

已连接，整个过程大约需要 2 分钟。

8) 部署成功后，页面中会显示该主机池/资源池的服务器类型、部署地址，主机池名称、该主机池/资源池下的所有主机、系统版本信息、文件和网络特征库信息及当前的连接状态，如下图所示。

9) 主机注册成功后，管理中心 “资产管理”->“虚拟机/终端”页面能够看到该机器，其实时防护状态正确。

10) 如果安装失败，主机状态会显示为“安装失败”，可点击“安装失败”字样查看失败原因。

通过脚本部署

(1) 使用 ssh 工具连接主机

(2) 有主机端使用命令 wget http://X.X.X.X:8080/agent/ics_agent.py 下载安装脚本

(3) 执行安装脚本，在如下图所示的交互式视图中输入相应的参数

```
[root@localhost ~]#
[root@localhost ~]# python ics_agent.py
/usr/bin/sudo
Please input IP address of management center:10.91.119.222
Please input host name [Default localhost.localdomain]:CentOS7.2
Do you want to install network module? yes/no [Default yes]:yes
Authorization type:
 1 server
 2 server with container
Please input 1 or 2 [Default 1 press Enter]:1
准备中...                          ################################# [100%]
正在升级/安装...
   1:ics-agent-common-3.5.3.101-1     ################################# [100%]
准备中...                          ################################# [100%]
正在升级/安装...
   1:ics-agent-net-3.5.3.1200-1       ################################# [100%]
准备中...                          ################################# [100%]
正在升级/安装...
   1:ics-agent-file-3.5.3.1000-1      ################################# [100%]
Starting ics-agent-file: kernel mode loaded
Done.
准备中...                          ################################# [100%]
正在升级/安装...
   1:ics-agent-integrity-1.0.0.12-1   ################################# [100%]
Register success.
[root@localhost ~]#
```

执行脚本

输入管理中心IP

输入主机名称

选择是否安装网络模块

选择许可证类型

参数说明：

Ip address of management center：管理中心 IP

host name ： 主机名，如果不输入则会使用默认值

install network module? yes/no [Default yes]：选择是否安装网络模块，默认为 yes

Authorization type ： 授权类型，标准版（standard）、高级版（container），默认为标准版

（4） 参数输入完成后，主机会从管理中心下载安装包，安装并注册

（5） 注册成功后，管理中心能够看到该机器，主机状态显示为“已连接”，使用脚本部署的主机会被默认添加至名称为“新注册主机”的主机池中。

（6） 资产管理”->“虚拟机/终端”页面也能够看到该机器，其实时防护状态正确

2.1.5 操作指南-控制中心版

2.1.5.1 首页

该区域主要显示版本相关信息等。此外还有几个功能入口：实时监控、警报、资产管理、安全策略、分析、报表、管理功能菜单。

管理-系统设置-特征库可以看到病毒特征库版本信息。

2.1.5.2 虚拟机/终端

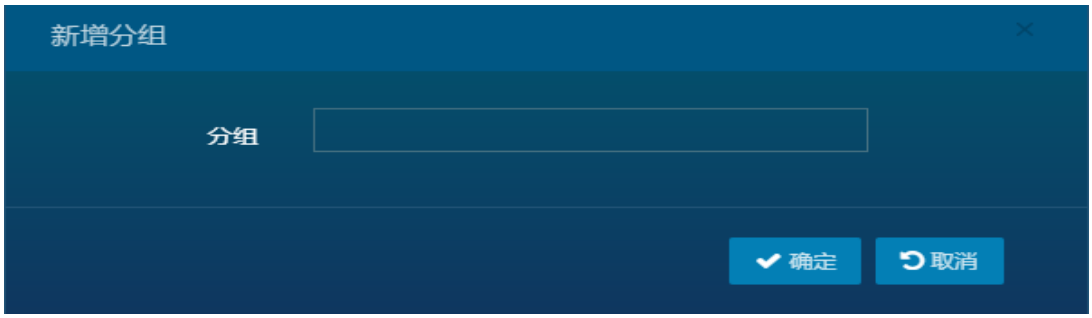
2.1.5.2.1 分组管理

将被管理的计算机进行分组，方便后期管理。可以针对分组定义匹配规则，也可以指定分组来查看实时监控，日志分析，生成报表等。
在多租模式的“所有项目”视图下，不显示分组信息。如果在多租模式进行分组管理，请先切换到对应的项目视图。
默认分组：系统默认创建，虚拟机如果没有匹配上分组规则或没有被指定分组，则全部属于默认分组。

- **新增**

1) 点击 资产管理->虚拟机/终端理->分组管理->新增

2) 在打开的“新增分组”对话框中输入分组名称，点击确定，左侧的分组列表中就能显示刚才创建的分组。

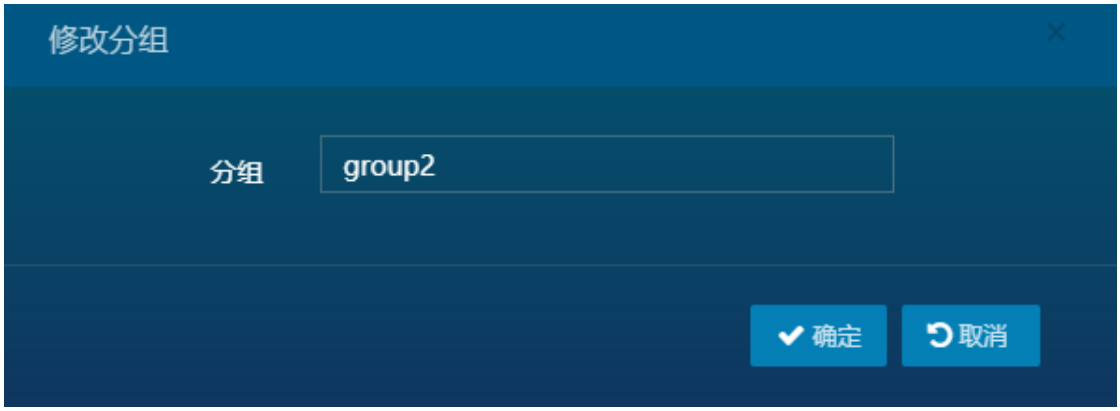


- **修改**

1) 在左侧分组列表选择要修改名称的分组

2) 点击 分组管理->修改

3) 在打开的“修改分组”对话框中输入分组名称，点击确定即可



- **删除**

1) 在左侧分组列表选择要删除的分组

2) 点击 分组管理->删除

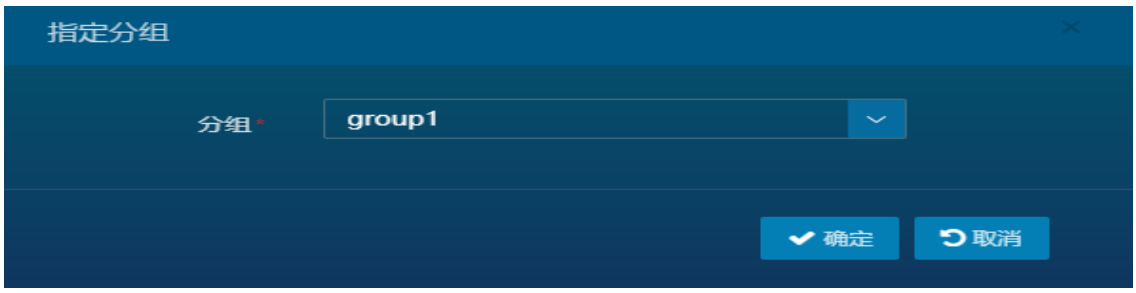
3) 在打开的“删除确认”对话框中点击确定即可

- **指定分组**

1) 选择要指定分组的虚拟机/终端

2) 点击 分组管理->指定分组

3) 在打开的“指定分组”对话框的分组列表中选择某个分组，点击确定即可



虚拟机的分组栏中有小手图标，表示是手动指定的分组

- **取消指定**

1） 选择要取消指定分组的虚拟机/终端

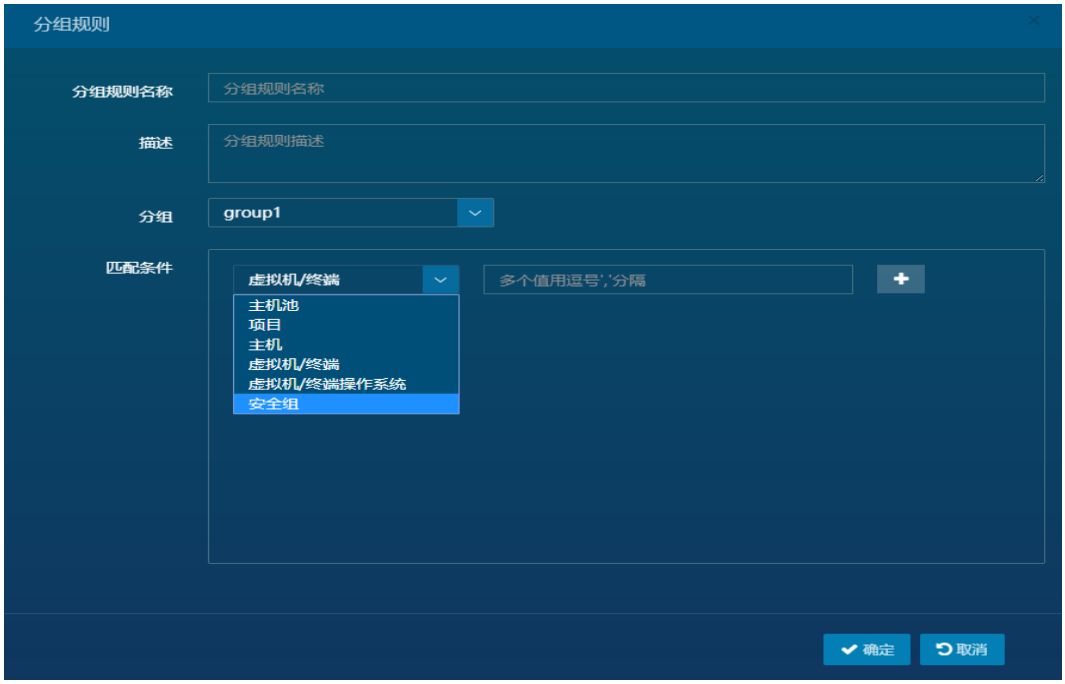
2） 点击 分组管理-> 取消指定

- **分组规则**
  - 新增

1） 在虚拟机/终端页面，点击 分组管理->分组规则

2） 在分组规则页面，点击 规则管理->新增

3） 在打开的“分组规则”对话框中输入分组规则的名称、描述、选择分组、配置匹配条件，点击确定即可



分组规则的匹配条件至少要包括下面的一项：

主机池： 虚拟机所在主机池的名称，可以配置多个，多个主机池名称之间用英文的逗号‘，’分隔。此条件为单租户模式下使用。

项目：虚拟机所在租户的名称，可以配置多个，多个项目名称之间用英文的逗号‘，’分隔。为多租户模式系统管理员视图下使用。多租户模式普通租户视图无法使用项目作为筛选条件。

主机：虚拟机所在主机的名称，可以配置多个，多个主机名称之间用英文的逗号‘，’分隔。

虚拟机/终端：虚拟机/终端名称，即**资产管理-虚拟机/终端**页面 虚拟机列表中显示的虚拟机名，可以配置多个，多个虚拟机名称之间用英文的逗号‘，’分隔。

虚拟机/终端操作系统：操作系统目前支持 Windows 和 Linux，由用户创建虚拟机指定。

安全组：openstack 虚拟机或 VMware NSX 环境中虚拟机所属的安全组

通过点击 + 来添加匹配条件，点击 − 来删除匹配条件。最多可添加 6 个匹配条件，且不能是同类型的匹配条件。

多个匹配条件之间是‘与‘的关系，即要满足所有匹配条件，才算匹配成功。
同一个匹配条件之间的多个值是‘或‘的关系，只要匹配上其中某个值，即算匹配成功。

■ 删除

1） 选择要删除的分组规则

2） 点击 规则管理->删除

3） 在打开的“删除确认”对话框中点击确定即可

■ 调整优先级

分组规则按从上至下的顺序进行匹配，调整分组规则优先级可以改分组规则的匹配结果。

1） 选择要调整优先级的分组规则

2） 点击 调整优先级-置顶/上移/下移/置底

■ 返回虚拟机/终端列表

在分组规则页面，点击 “返回虚拟机/终端列表”按钮即可返回虚拟机/终端页面

主机添加成功后，虚拟机页面会显示主机中所有虚拟机信息。包括虚拟机名称、虚拟机状态、虚拟机操作系统、安全配置、所属主机池或项目、所属主机、实时防护状态和安全检测状态。

主机添加成功后，虚拟机页面会显示主机中所有虚拟机信息。包括虚拟机名称、虚拟机状态、虚拟机操作系统、安全配置、所属主机池或项目、所属主机、实时防护状态和安全检测状态。

以下是虚拟机列表中虚拟机状态和和实时防护状态说明：

虚拟机状态		虚拟机正在运行
		虚拟机被挂起
		虚拟机被停止
实时防护状态		实时防护开启
		实时防护关闭
		虚拟机/终端未运行
		安全防护功能未开通
		VMware 安全虚拟机
		管理中心
		此图标表示 3 种状态 1.如果对应的虚拟机是 VMware 虚拟化平台中的 Linux 虚拟机，则此图标表示

		“虚拟机/终端未安装 NSX File Introspection/vShield 驱动程序或代理安全组件，请点击并根据提示进行安装” 2.如果对应的虚拟机是 VMware 虚拟化平台中的 Windows 虚拟机，则此图标表示“NSX/vShield Manager 和 ESXi 主机时间不同步或虚拟机/终端可能没有安装 NSX File Introspection/vShield 驱动程序” 3.如果对应的虚拟机是非 VMware 虚拟化平台中的虚拟机，则表示”虚拟机没有安装消息中心，请点击下载“消息中心”并为虚拟机安装”

虚拟机处于挂起或停止状态时，管理中心是无法获取其实时防护状态的，所以会显示为空

2.1.5.2.2 安全策略

1）默认安全配置

系统中有两种默认安全配置，即 Linux 安全配置、Windows 安全配置。系统会根据虚拟机的操作系统为其自动分配对应的安全配置。

2）指定安全配置

在虚拟机页面，管理员也可以手动为虚拟机指定安全配置。手动指定的安全配置会优先于自动匹配安全配置。

a） 在虚拟机列表选中一个或者多个虚拟机

b） 点击“**安全策略 > 指定安全配置**”，在弹出页面选择安全配置，然后确认。

c） 这些虚拟机将使用指定的安全配置，虚拟机列表的“安全配置”前有一个小图标 表示其由手动指定。如下图所示

3）取消指定

手动指定安全配置后，也可以取消指定。

a） 在虚拟机列表选中一个或者多个虚拟机

b） 点击“**安全策略 >取消指定**”即可恢复到默认的安全配置

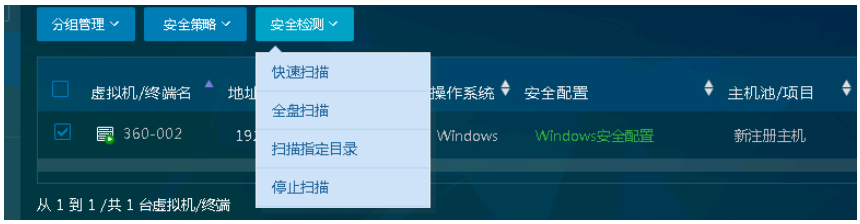
4）恢复默认安全功能

a) 在虚机列表中选中一个或多个虚拟机

b) 点击“安全策略 > 恢复默认安全功能”，虚拟机的安全功能会恢复到初始状态。

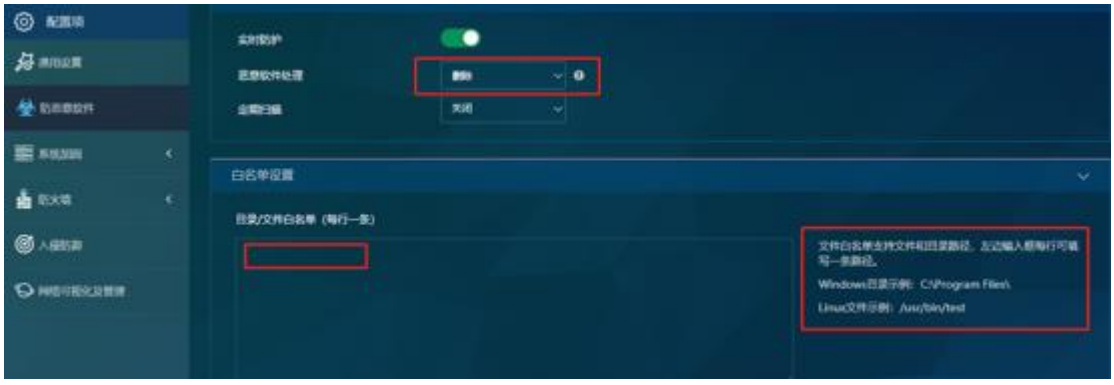
2.1.5.2.3 扫描指定目录

进入管理中心 资产管理-虚拟机/终端 页面，将需要扫描的虚拟机的安全配置中的实时防护状态关闭，恶意软件处理选择删除/隔离；在虚拟机页面，选择对应的虚拟机，点击 安全操作->快速扫描。



2.1.5.2.4 目录文件白名单

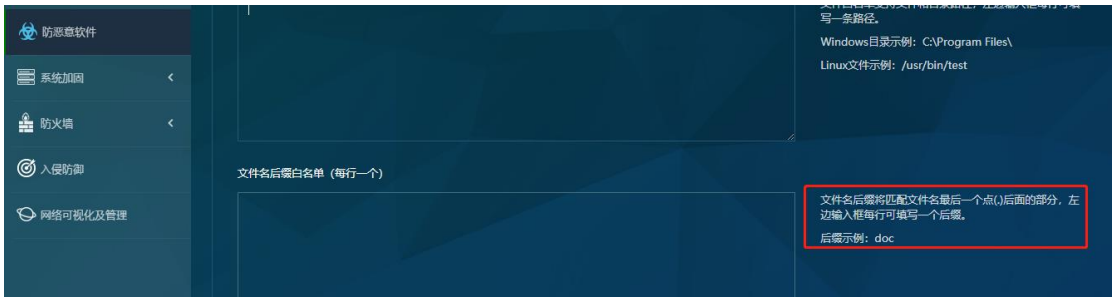
进入 管理中心 资产管理-虚拟机/终端 页面，将需要扫描的虚拟机的安全配置中的实时防护状态打开，恶意软件处理配置为删除，目录/文件白名单配置。



2.1.5.2.5 文件后缀名白名单

进入 管理中心 资产管理-虚拟机/终端 页面，将需要扫描的虚拟机的安全配置中的实

时防护状态打开，恶意软件处理配置为删除，文件后缀名白名单配置



2.1.5.2.6　排序/过滤/搜索

1）虚拟机列表排序

点击虚拟机列表头中右侧的 ，可以按照虚拟机/终端 名、操作系统、安全配置、主机池/项目、主机对虚拟机列表进行排序，方便管理员查看。

2）虚拟机过滤

虚拟机/终端页面可以根据实时防护状态来对虚拟机进行过滤，方便用户查看。

3）搜索虚拟机

管理员可以按照虚拟机名、操作系统、安全配置和主机对虚拟机进行搜索。支持模糊匹配、不区分大小写。

2.1.5.3 安全配置

2.1.5.3.1 默认安全配置

安全配置是防护系统针对每台虚拟机的所有安全设置的集合，包括防恶意软件设置，定义好安全配置后， 可以将它应用到多台虚拟机。可以定义规则自动匹配，也可以手动为虚拟机指定安全配置。

系统默认安全配置：系统中有两种默认安全配置，即 Linux 安全配置和 Windows 安全配置。当主机添加成功后，管理中心会根据主机中虚拟机的操作系统，为其自动匹配默认的安全配置。

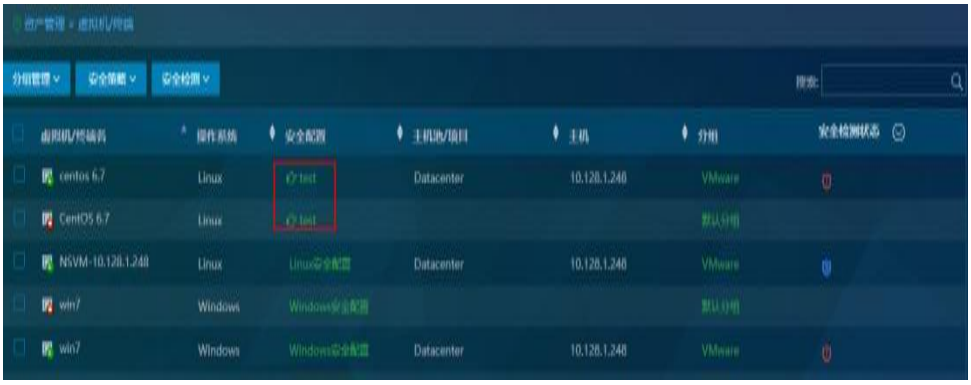
1）指定安全配置

在虚拟机页面，管理员也可以手动为虚拟机指定安全配置。手动指定的安全配置会优先于自动匹配安全配置。

d）在虚拟机列表选中一个或者多个虚拟机

e）点击“**安全策略 > 指定安全配置**”，在弹出页面选择安全配置，然后确认。

f）这些虚拟机将使用指定的安全配置，虚拟机列表的“安全配置”前有一个小图标 表示其由手动指定。如下图所示



2）取消指定

手动指定安全配置后，也可以取消指定。

c）在虚拟机列表选中一个或者多个虚拟机

d）点击“**安全策略 >取消指定**”即可恢复到默认的安全配置

2.1.5.3.2　编辑安全配置

编辑安全配置页面包括 7 个选项卡，分别在每个选项卡内进行相应的设置。

- **通用设置**

名字：　规则名称，支持中文名，是必选项。

描述：　可选项。

- **防恶意软件**

a）实时防护：　如果打开实时防护 

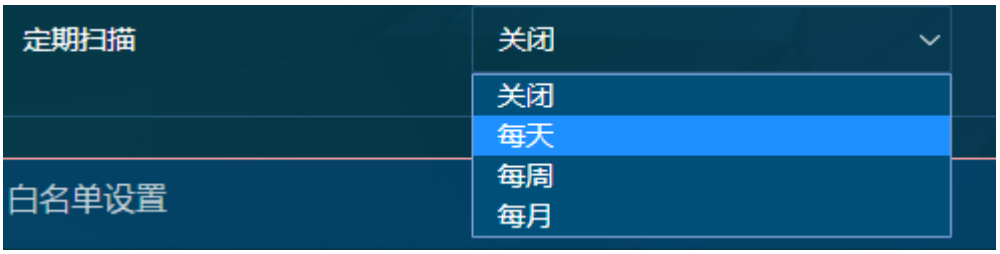
，应用该安全配置的虚拟机将受到实时的防恶意软件防护，虚拟机列表中的实时防护状态会变为 

如果关闭实时防护 

，应用该安全配置的虚拟机不会受到实时的防恶意软件防护，虚拟机列表中的实时防护状态会变为  ，默认是打开状态。

b）恶意软件处理：如果在虚拟机中检测到病毒，系统提供了以下 4 种方式对病毒进行处理

c）定期扫描：可以选择定期对虚拟机进行全盘扫描。时间可以是每天，每周或者每月的具体某个时间点，默认是关闭状态。



注：只有虚拟机为开启状态才会进行定期扫描。

例如，配置定期扫描时间为每天 15:00，则如果有虚拟机在 15:00 到 16：00 这段时间内从挂起或关闭状态变成开启状态，虚拟机起来后也会进行定期扫描。

d）文件白名单： 将文件夹或者文件路径加入白名单，安全模块将不对这些文件进行扫描和检测。匹配时采用模糊算法，如果要扫描的文件全路径中包含有白名单中的任何一项，则被算作匹配。 编辑框中每行填入一个白名单路径。

例如:”C:\Program Files\”将匹配文件夹及其下面的所有文件和文件夹。

e）文件名后缀白名单： 如果文件名的后缀匹配这个白名单中任何一项，将跳过扫描和检测。 可以配置多个文件后缀，每个文件后缀之间用换行符进行分隔。

f） 仅扫描指定目录设置：如果选中“仅扫描下列目录”复选框，可以把扫描目录限制到指定的目录范围。同时可以把指定目录范围应用到手动全盘扫描，实时扫描和定期扫描中的一项或者多项。

g） 仅扫描包含指定后缀名的文件：如果选中“仅扫描包含下列后缀名的文件”复选框，可以限定只扫描特定文件类型。同时可以把指定文件类型应用到手动全盘扫描，实时扫描和定期扫描中的一项或者多项。

2.1.5.3.3 搜索安全配置

可以根据安全配置的**名称/描述/保护的机器**来搜索安全配置，支持模糊搜索

2.1.5.3.4 复制、删除安全配置

在安全配置列表中选择需要复制或删除的安全配置，点击**复制/删除**按钮即可。

2.1.5.4 用户管理

防护系统管理中心支持多用户和多角色的管理。系统内置 admin 和 audit 角色，用户可以根据需求创建新的角色。同时系统内置 admin 用户，admin 用户不能删除。

2.1.5.4.1 用户管理

新增用户： 在**用户管理**标签页点击“**新增**“按钮，在打开的”用户管理“对话框中填写各个选项，其中用户名和密码是必填项，根据需要选择合适的“角色”，点击确定按钮。

密码复杂度 ：新增用户时有密码复杂度要求，要求密码必须至少包含六个字符且需要采用以下四类字符中的三类：英文大写字符（A-Z)、英文小写字符（a-z)、10 个基本数字（0-9)和非字母字符（!、$、#、% 等)。
编辑用户：如果想要修改用户的相关参数，在用户列表中点击需要修改参数的用户名，在打开的‘**用户管理**‘对话框中修改即可

删除用户：选中需要删除的用户，点击“**删除**“按钮。
搜索用户：可以根据用户名、邮箱地址和描述进行搜索，支持模糊搜索，不区分大小写。
同一账号多次登录管理：

a） 多人同时用相同账号登陆，提醒用户其他地方有人用相同账号登陆（包括　先登录用户，和后登录用户）

b） 用户可以查看当前使用相同账号登录会话的信息，包括登录 IP，登录在线时间

c） 用户可以踢出已登录会话，让其强制退出登录

2.1.5.4.2　角色管理

新增角色： 在**角色管理**标签页点击“**新增**“按钮，在打开的”角色管理“对话框中填写角色名，并根据需要选择合适的权限，点击确定按钮。

编辑角色：如果想要修改角色的相关权限，在角色列表中点击需要修改的角色名，在打开的‘**角色管理**‘对话框中修改即可

删除角色：选中需要删除的角色，点击“**删除**“按钮。 不能直接删除已经被用户关联的角色，必须先删除所有关联用户，然后再删除该角色。

3. 常见问题

1. 为什么管理中心实时监控中一直没有数据？

主机安全组件会把流量日志和安全事件发送回管理中心，由管理中心进行处理后最终在实时监控中显示。由于实时监控的数据具有实时性要求，如果收到的日志时间和当前时间误差大于 2 小时，管理中心将丢弃这些日志。这样就会导致实时监控中没有数据。通常是由于主机和管理中心的系统时间没有同步造成的，解决办法是同时在主机和管理中心上打开 NTP 时间同步机制。

注： 如果管理中心与主机时间不同步，管理中心会产生对应的警报。

2. 管理中心重新配置网卡或者克隆之后，ip 地址无法获取或配置失败怎么办？

新增的网卡的信息与旧网卡的配置不匹配，导致网络服务启动失败，接口无法获取 ip 地址。只要在管理中心运行“configure network reset”命令和“reboot”命令，在重启之后，重新配置 ip 地址即可生效。

3. 浏览器相关

防护系统支持近两年内发布的大部分浏览器。

然而由于一些虚拟化特性，部分虚拟机不支持 WebGL. 故这些浏览器查看具有 3D 效果的组件时，不能正常显示。建议使用物理机，高阶一些的浏览器。

浏览器/类型	物理机	虚拟机	备注
IE	IE9、IE10、IE11 兼容	IE9、IE10、IE11 兼容	IE 10 2013 年 2 月发布， IE 11 2014 年 1 月发布
firefox	Firefox 31.0 兼容	Firefox 31.0 兼容	31.0 2014 年 8 月发布
chrome	Chrome 35.0 兼容	Chrome 35.0 兼容	35.0 2014 年 6 月发布

4. 管理网络和计算网络是相互隔离的，虚拟机连的是计算网络，无法连接管理网络，但是又需要与管理中心进行通信，如何解决？

在创建管理中心时，需要添加两个网卡，分别连接管理网络和计算网络。管理中心安装成功后，可进入 CLI 配置其中一个网卡为管理口。输入命令：configure network management interface 并回车，在下图所示的向导中输入对应的网卡编号即可

```
>
> configure network management interface
Interfaces:
-----------------------------------------------------
1. eth0 10.128.1.40
2. eth1 192.168.145.17
-----------------------------------------------------
There are 2 interfaces above in the system.
Please input the interface number(0 for no management interface):1
Interface eth0 has been set as management interface
Stopping vmsec controller:                                 [  OK  ]
Starting vmsec controller:                                 [  OK  ]
>
>
```

只有配置为管理口的接口才能访问管理中心的页面，如果不配置的管理口的话，则通过两个接口均能访问管理中心页面。

5. 使用 windows 系统普通权限用户安装安全组件时报错。

原因：被 windows UAC 拦截，需要添加注册表配置。

解决方法：以管理员身份运行 cmd，输入以下命令：

reg add "HKLM\Software\Microsoft\Windows\CurrentVersion\Policies\system" /v LocalAccoutTokenFilterPolicy /t REG_DWORD /d 1 /f

保存成功即可。

```
C:\Windows\system32>reg add "HKLM\Software\Microsoft\Windows\CurrentVersion\Poli
cies\system" /v LocalAccoutTokenFilterPolicy /t REG_DWORD /d 1 /f
操作成功完成。
```

附录：管理中心 CLI 命令行参数说明

远程 SSH 访问管理中心，将进入 CLI 命令行界面。在命令行中输入 ?，可以查看可用的 CLI 命令列表；输入命令时使用 Tab 进行命令的补全。

1) configure

```
> configure

backup    backup to server.
date      Configure system date and save to CMOS
hostname  Change the hostname.
language  Language configuration.
module    Module configuration
network    network configuration
restore   restore data from backup.
```

Configure 命令中有 7 个子命令

Configure date <date><time>, 手动输入日期和时间

```
> configure date 2017-04-28 11:01:12
date: 2017-04-28 11:01:12
```

configure date ntp <server1> [server2]配置 NTP 服务器来校准时间，server1 是必填项，server2 是可选项

```
> configure date ntp cn.pool.ntp.org
```

configure hostname <newname>配置机器名称

configure language <en | zh> 修改系统后台数据的语言。支持中文和英文，默认为中文。

configure module network <onoff>打开或关闭管理中心的网络模块

configure network 配置网络相关参数，其下有 4 个子命令

```
> configure network

dns     Configure network DNS settings
ip      Configure network interface ip static address
reset   Network: NIC data may change.
route   Configure route settings
```

configure network dns <dns1> [dns2]，配置管理中心的 dns server

configure network ip dhcp [ethname] ，配置管理中心自动获取 IP

configure network ip static [ethname] <ip><mask> [gw] ，为管理中心配置静态 IP

configure network reset，清空网络配置并重启网络

configure network route，添加或删除路由

a) configure network route add <ip><mask> [gw] [ethname]

b) configure network route adddefault <ip> [ethname]

c) configure network route del <ip><mask> [gw] [ethname]

d) configure network route deldefault

configure backup 和 configure restore 分别是指将管理中心数据备份至 NFS 服务器和从 NFS 服务器恢复数据到管理中心

2) **entershell**

输入密码即可进入管理中心后台

3) **exit**

退出 CLI

4) **ping**

ping <dest> [ethname]指定从某个网卡 ping 目录地址

5) **reboot**

重启管理中心

6) **reset**

重置管理中心的所有参数

7) **show**

show date 查看系统时间

show interface 查看管理中心的接口信息

show language 查看管理中心后台数据的语言

show network 查看管理中心的网络参数

show routes 查看系统路由

8) **shutdown**

管理中心关机

9) **traceroute**

traceroute [-h hops] <dest>， 探测从管理中心到目标地址之间的路径

10) **vmtool**

vmtool install 为管理中心安装 vmtool（用于 H3C 平台）