



天翼云 · 微隔离防火墙

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	5
1.1 产品定义	5
1.2 术语解释	5
1.3 产品功能	6
<i>可视化业务拓扑</i>	<i>6</i>
<i>面向业务策略管理模型</i>	<i>6</i>
<i>自适应微隔离技术</i>	<i>6</i>
<i>内部流量分析</i>	<i>6</i>
1.4 产品优势	6
1.5 应用场景	7
2 购买指南	8
2.1 规格	8
2.2 价格	8
2.3 订购	9
2.4 升级	12
2.5 续订	13
2.4 到期效果	13
3 操作指南	14
3.1 登录管理中心 (QCC)	14
3.2 管理中心 (QCC) 授权	15
3.2.1 导出识别文件	15
3.2.2 获取授权文件	16
3.2.3 导入授权文件	16

3.3	可视化分析使用说明	18
3.3.1	首界面/业务拓扑基本功能说明	18
3.3.2	业务拓扑使用说明	22
3.3.3	连接分析使用说明	27
3.4	创建工作组	28
3.4.1	新建组标签	28
3.4.2	创建工作组	29
3.5	接入工作负载（BEA 端）	30
3.5.1	创建授权码	30
3.5.2	接入工作负载	32
3.6	工作负载管理模块	32
3.6.1	工作组	33
3.6.2	工作负载	36
3.6.3	标签管理	38
3.7	安全策略管理模块	38
3.7.1	策略与策略集	38
3.7.2	服务对象	40
3.7.3	地址对象	42
3.7.4	更新发布	44
3.7.5	发布记录	44
3.8	告警与事件	45
3.8.1	告警规则	46
3.8.2	操作日志	46
3.8.3	系统日志	47
3.9	系统配置	47
3.9.1	系统管理	47

3.9.2 虚拟中心管理	49
3.9.3 账户管理	49
4 常见问题	51
Q:WINDOWS 系统在安装客户端时，提示访问被拒绝，如下图所示：	51
Q:安装过程中无报错，但管理中心中未出现新安装的云主机	51
Q:使用 IE 浏览器访问产品管理页面时，一直显示加载中	52
Q: 自适应微隔离产品需要对外提供那些端口访问，才能正常工作？	52
Q:自适应微隔离产品的管理控制台登录方式？	52
Q: 自适应微隔离 WEB 控制台必需使用何种浏览器？	52
Q: 自适应微隔离 WEB 控制台初始的登录用户名密码是什么？	52
Q: 自适应微隔离 WEB 控制台密码被锁定了怎么办？	53
Q: 自适应微隔离 WEB 控制台忘记登录密码怎么办？	53
Q: 如何获取自适应微隔离的客户端安装命令？	53
Q: 为什么配置了策略工作负载没有启动防护的作用？	56
Q: 业务拓扑图的红色线和绿色线都代表什么？	56

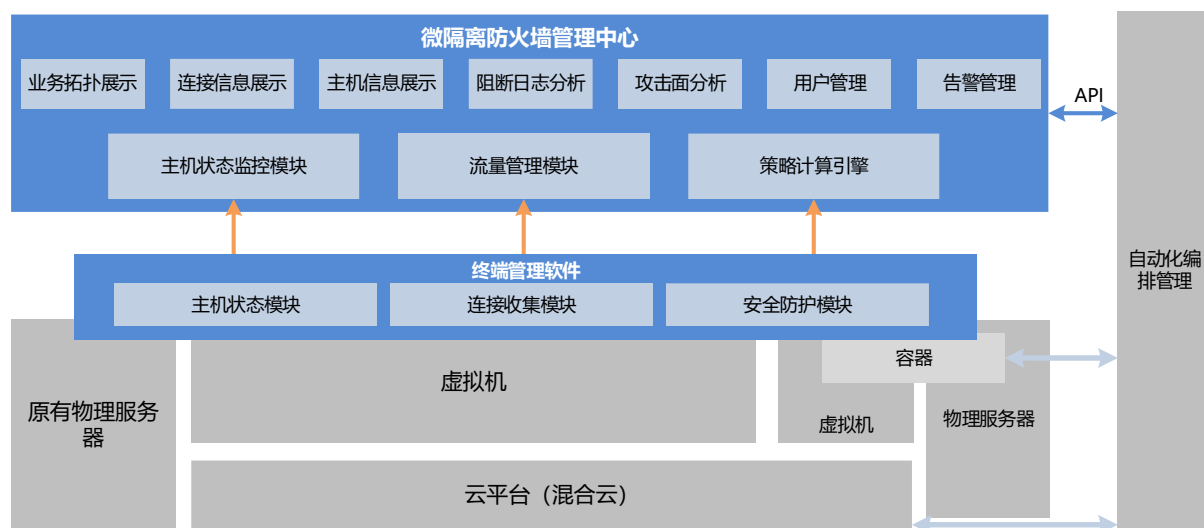
1 产品介绍

1.1 产品定义

微隔离防火墙（CT-MIFW Micro-isolation Firewall）可实现集中可视化管理云主机安全策略，绘制内部业务流量拓扑，帮助用户快速便捷地实现细粒度的访问控制。与云下一代防火墙互补，实现纵深防御。

1.2 术语解释

微隔离防火墙的总体技术架构由两部分组成，一部分是集中的蜂后安全计算中心 QCC（Queen Compute Center，以镜像方式提供），一部分是安装在主机上的蜂群安全管理终端 BEA（Bee Enforcement Agent，由 QCC 获取安装命令），。BEA 持续的监控主机 context 和一些运行时统计信息并将这些信息不断传送给 QCC。QCC 根据来自 BEA 的 context 持续进行策略计算，并将生成策略下发给 BEA，由 BEA 完成对主机的策略更新。



产品技术架构图

微隔离：Micro-segmentation，Gartner 定义的一种云安全技术，又译为微分段。主要解决软件定义数据中心中主机间的访问控制与可视化。

南北向流量：进出互联网边界的流量称为南北向流量。

东西向流量：数据中心中不同服务器之间的流量称为东西向流量。

1.3 产品功能

可视化业务拓扑

无论是私有云、公有云还是混合云环境，微隔离防火墙均能为您统一绘制出一张完整的业务流量拓扑图，并通过交互式设计，提供针对流量和策略更加便捷的钻取与控制能力。

面向业务策略管理模型

提供一种独特的应用及云主机定义方法，并建立一套简化的、可适应的、接近自然语言的策略模型；上帝视角对策略进行规划，并通过页面直接下发规则，保持安全运维人员的思维在同一层面。

自适应微隔离技术

微隔离防火墙能够根据数据中心内部的变化而自动调整安全策略，结合微隔离技术，能够实现自适应的端到端的精细化访问控制。

内部流量分析

产品自动学习云主机访问流量，并提供多维度对流量的分析能力，结合告警功能，可帮助您快速发现勒索病毒传播、横向移动、恶意扫描等内部异常流量。

1.4 产品优势

流量可视化监控：支持内网云主机互访流量分析、业务可视化拓扑，全面了解资产的信息和访问关系，从而及时发现异常流量。

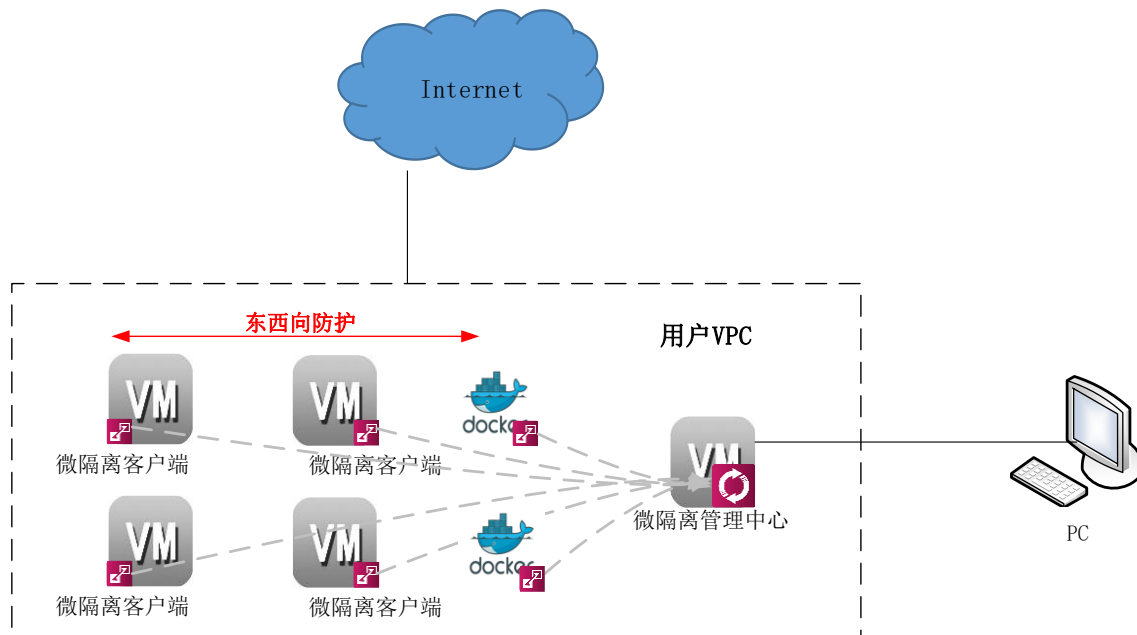
微隔离访问控制：支持内部云主机之间的微隔离访问控制（东西向），基于拓扑设置安全策略、可减少内部安全策略总数的 90%。

安全策略可视化管理：在业务拓扑中利用红绿线标识符合策略的流量及不符合策略的流量，并支持查看流量阻断日志。

自适应策略调整：在业务迁移、弹性拓展等场景下，可自动调整安全策略，并支持 API 自动化编排。

混合云统一安全管理：对于混合云客户，产品支持跨云平台的统一流量可视化及安全策略统一。

1.5 应用场景



该拓扑图包含物理服务器、本地数据中心虚拟机、容器、公有云、灾备云等多个场景，用户根据实际环境选择其中全部或部分进行部署。

政企网站病毒与异常行为发现及防护

及时发现勒索病毒传播、横向平移等异常行为；对异常行为实时阻断，规避潜在的风险端口，缩小攻击面。

政企业务系统等保合规

产品可协助用户满足等保 2.0 中“应在关键网络节点处检测、防止或限制从内部发起的网络攻击行为”、“应允许云服务客户设置不同虚拟机之间的访问控制策略”等要求。

互联网、金融网站业务可视化及端口管理

业务主机开放了多种业务端口服务，需要可视化业务流量与服务端口，实现访问关系授权与端口台账。

2 购买指南

2.1 规格

微隔离防火墙以镜像方式提供服务，用户需要一台云主机安装产品镜像，然后申请最大资产数和使用时间的授权。

微隔离防火墙按照用户保护的最大终端数量定义了最大资产数，分为三档依次为 20L、50L、100L、200L、400L、800L。各档最大资产数对应管理中心云主机配置要求参照下表，

序号	最大资产数	管理中心主机配置
1.	20	1 核 2G, 60G 数据盘
2.	50	1 核 4G, 100G 数据盘
3.	100	2 核 4G, 200G 数据盘
4.	200	2 核 4G, 200G 数据盘
5.	400	4 核 8G, 300G 数据盘
6.	800	8 核 16G, 400G 数据盘

2.2 价格

产品规格（防护主机台数）	标准价格（元/月）
20	1700
50	4200
100	8300
200	16600
400	29900
800	59800

备注：针对一次性包年付费服务，标准价格按照如下优惠政策进行操作，且在订购期间不允许退订服务。

一次性付费 1 年	一次性付费 2 年	一次性付费 3 年
包月标准价格 *12*85%	包月标准价格 *24*85%	包月标准价格 *36*85%

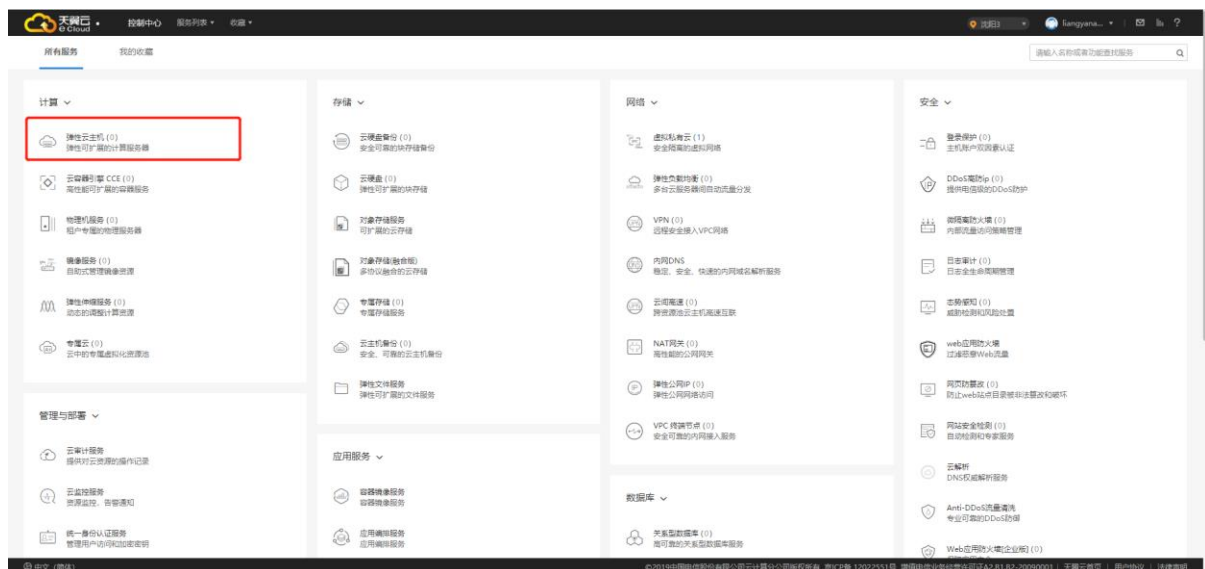
2.3 订购

微隔离防火墙以镜像方式承载，订购前需要开通一台云主机承载业务，然后再购买授权。操作步骤如下，

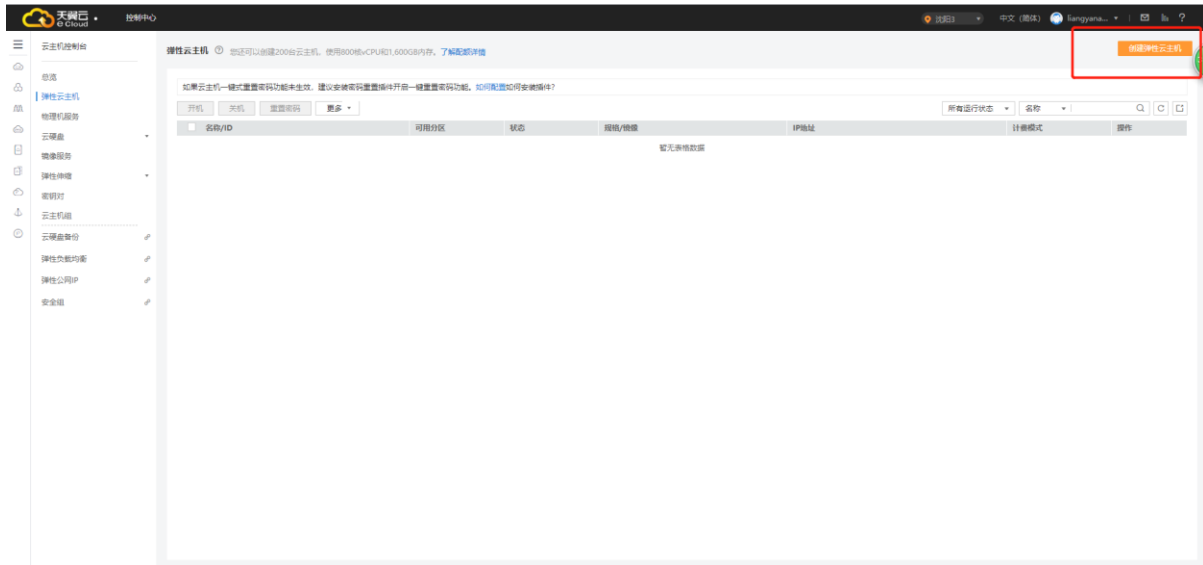
1、进入天翼云官网，点击右上角【控制中心】。



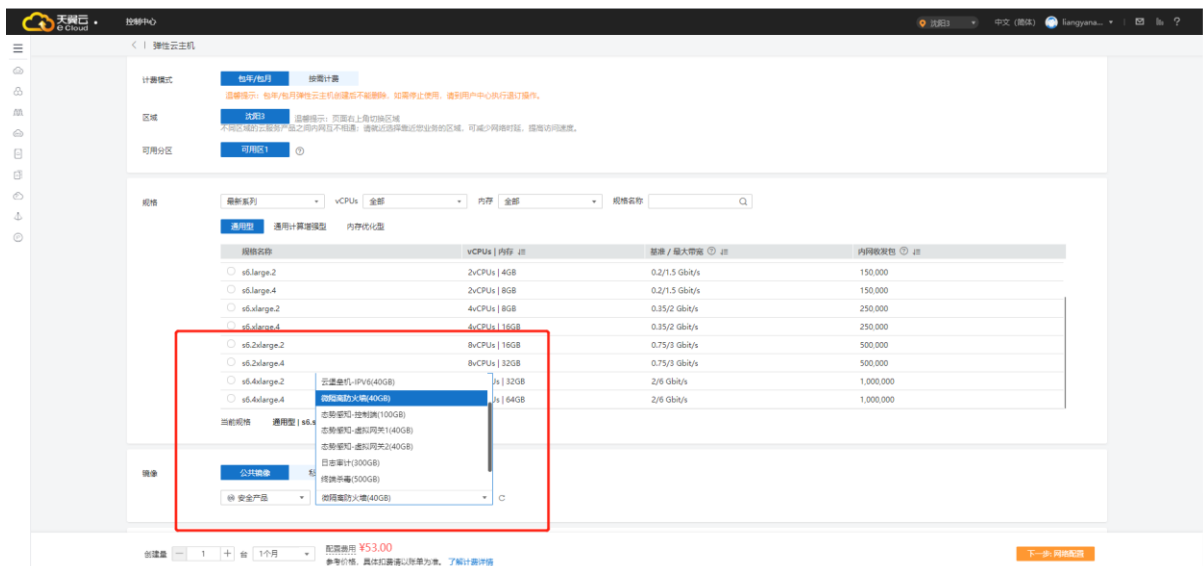
2、点击【弹性云主机】



3、点击【创建弹性云主机】



4、按需选择相应的云主机规格，需注意：在选择公共镜像时，选择安全产品中的微隔离防火墙。



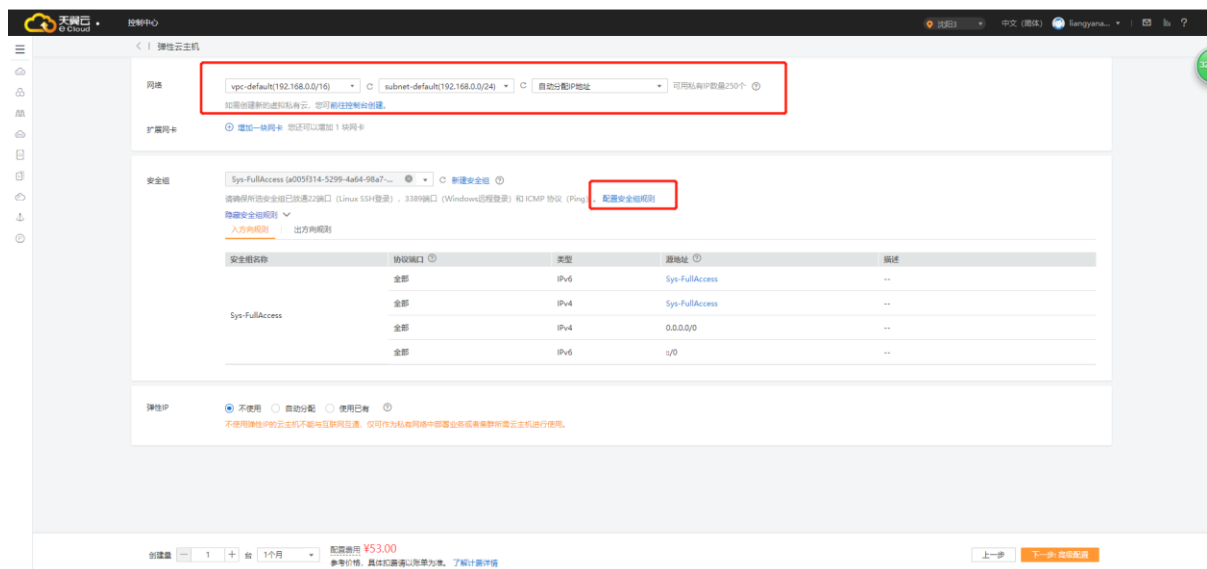
5、云主机需开放端口：10443、6443、8000、60001、60011、60021、60031 端口。6443 为 WEB 控制台访问端口，10443 端口为后台管理使用的端口，8000 安装 agent 的访问端口，60001、60011、60021、60031 为 agent 接入自适应微隔离管理中心的使用端口。

开放端口操作：

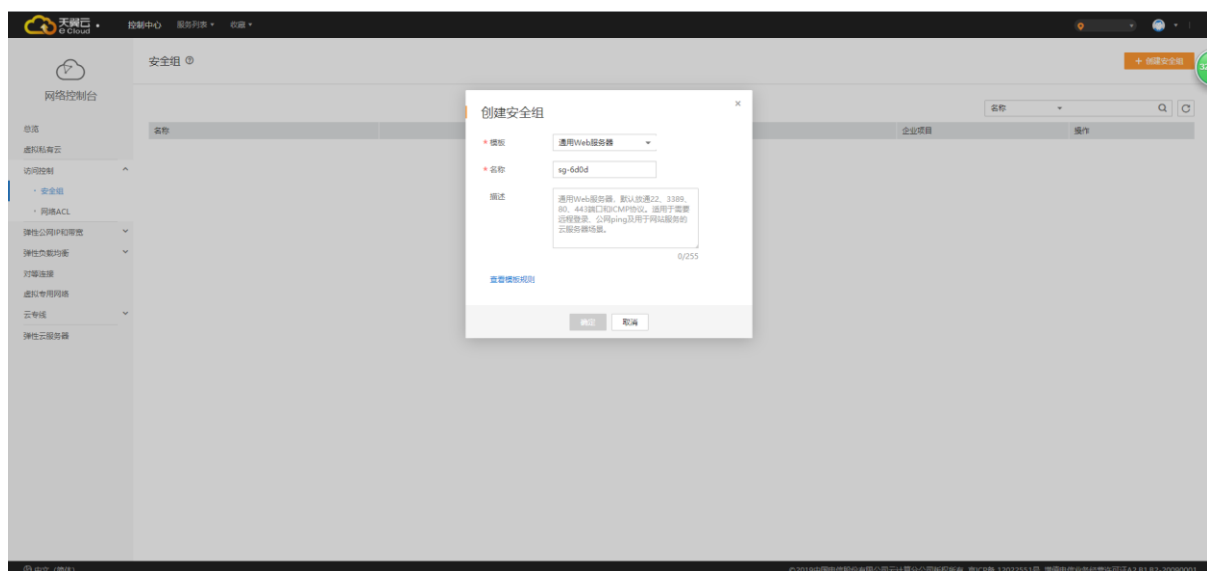
1) 点击上图的【下一步：网络配置】进行配置



2) 进入【配置安全规则】



3) 点击【创建安全组】



6、在创建完成云主机后，在【控制中心】中选择安全项中的【微隔离防火墙】。点击小购物车“🛒”进入订购页面。

7、设置实例名称，选择需要微隔离防护的云主机数量，上传识别文件（文件的获取参照 3.2.1 倒出识别文件），选择订购时长，勾选服务协议，即可提交订购。本产品的授权过程需要 1-2 个工作日的时间完成，完成授权后会生成对应的实例项，授权文件可以在 console 页面的实例信息中下载，我们也会邮件通知授权文件。

订购微隔离防火墙

订购须知:

- 1、本产品是以镜像方式提供服务，须另购买一台云主机进行部署。本页面购买的是微隔离防火墙的授权，请确保已安装微隔离防火墙控制中心再进行订购。
- 2、请确保已在安全组开放了443、10443、6443、8000、60001、60011、60021、60031端口。
- 3、本产品授权一经订购立即生效，除不可抗力因素外，不支持退订。

实例名称:
请填写实例名称

最大资产数: 20(台) 50(台) 100(台) 200(台) 400(台) 800(台)
选择需要防护的云主机的台数

软件识别文件: 上传文件 **需上传license.req文件**
制作授权需要，请上传软件识别文件，获取方法可以查看 [《微隔离防火墙产品授权》](#)

购买时长: 1个月 2个月 3个月 4个月 5个月 6个月 7个月 8个月 9个月 10个月 11个月 1年 2年 3年
请选择购买时长
1年 8.5折 2年 8.5折 3年 8.5折

费用总计 **2550.00** 元 立即订购

我已阅读，理解并接受 [《微隔离防火墙产品使用协议》](#)

2.4 升级

升级操作是在 console 页面产品实例列表进行的，点击【升级】会弹出升级配置页面，用户可以选择升级到的新规格。升级的规格默认有效期与原实例保持一致。

实例名称	授权数量	授权文件	开通时间	截止时间	操作
QCC-t0es	20		2020-05-15 17:34:05	2020-06-15 17:34:05	续订 升级
QCC-2bnj	5673160c4d594edaa19661 94da784c9d	下载	2020-02-13 10:30:33	2020-03-13 10:30:33	续订 升级
QCC-sy1n	20		2019-12-12 17:20:18	2020-01-12 17:20:18	续订 升级
QCC-dhye	20	bssupload 下载	2019-10-18 14:56:20	2019-11-18 14:56:20	续订 升级

共 4 条 10条/页 < 1 > 前往 1 页

升级

实例名称: QCC-t0es

当前最大资产数: 20

选择升级规格: 20(L) 50(L) 100(L) 200(L) 400(L) 800(L)

只能升规格，不能降规格。更新规格后为运行顺畅须建议对应变更云主机规格。升级受理完成后，请到控制台及时下载最新授权文件导入激活。

确定 我已阅读，理解并接受 [《微隔离防火墙产品使用协议》](#)

2.5 续订

续订操作是在 console 页面产品实例列表进行的，点击【续订】会弹出续订配置页面，续订是在原实例到期的基础上增加的有效时间。

续订 ×

实例名称: QCC-t0es

购买时长: 1个月 2个月 3个月 4个月 5个月 6个月 7个月 8个月 9个月 10个月 11个月 1年 2年 3年
8.5折 8.5折 8.5折

当前服务截止日期为: 2020-06-15 17:34:05

续订受理完成后, 请到控制台及时下载最新的授权文件

费用总计: **850.00**元

我已阅读, 理解并接受《微隔离防火墙产品使用协议》

2.4 到期效果

产品授权到期前 7 天会在登录页面给出到期提醒，产品到期后，配置的策略依然有效，但是无法登录平台进行调整。建议不计划继续试用本产品的用户，在产品到期前将所有策略关闭掉。

3 操作指南

用户确保已经成功安装平台的管理中心（QCC），开放了 10443、6443、8000、60001、60011、60021、60031 端口，并且安装客户端的工作负载与管理中心网络可达。6443 为 WEB 控制台访问端口，10443 端口为后台管理使用的端口，8000 安装 agent 的访问端口，60001、600011、60021、60031 为 agent 接入自适应微隔离管理中心的使用端口，

3.1 登录管理中心（QCC）

产品采用 web 页面进行管理及操作，在浏览器输入“https://+管理地址：映射的端口”即可进入登录界面，

系统默认的后台管理登录地址为 <https://+管理 IP: 10443>,

系统默认的日常操作登录地址为 <https://+管理 IP: 6443>


默认密码：admin@338

默认密码在受理完成后，产品控制台实例列表中下载，如下图所示。

微隔离防火墙 购买微隔离防火墙

实例名称	授权数量	授权文件	服务开始时间	服务到期时间	操作
QCC-sy1n	20		2019-12-12 17:20:18	2020-01-12 17:20:18 已过期	升级 续订
QCC-dhye	20	bssupload 下载	2019-10-18 14:56:20	2019-11-18 14:56:20 已过期	升级 续订

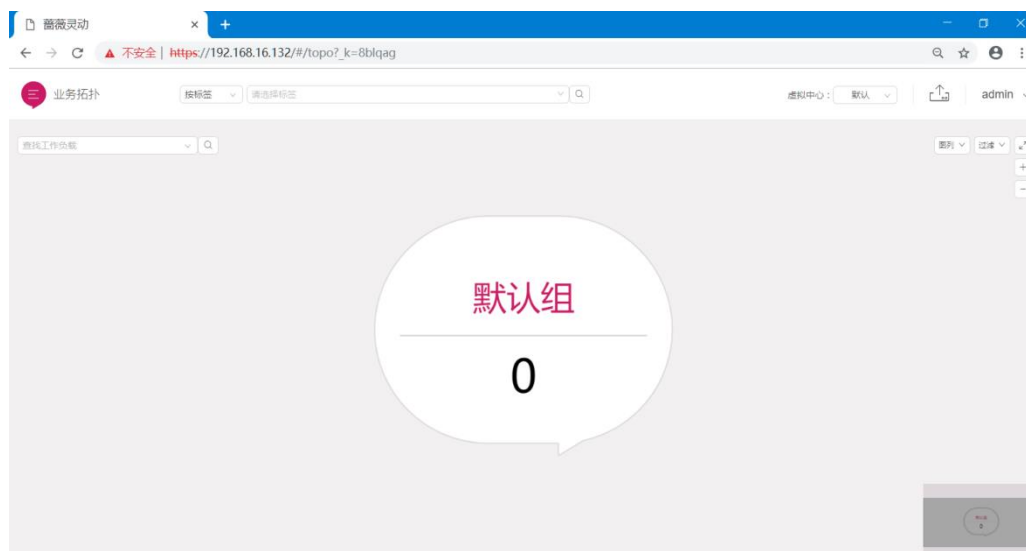
共 0 条 < 1 > 前往 页

以 6443 为例，输入用户名及密码后点击确定或输入“回车”即可完成登陆。其中密码输入框处的  标识，点击可查看密码。



密码输入错误后会有剩余输入次数的提示，默认为 5 次，超过后将会被锁定。admin 被锁定后只能联系厂家解锁，其他用户被锁定，可登录 admin，在系统管理中解锁。

登录完成，进入平台（V2.13）首界面，首次登录时，界面如下

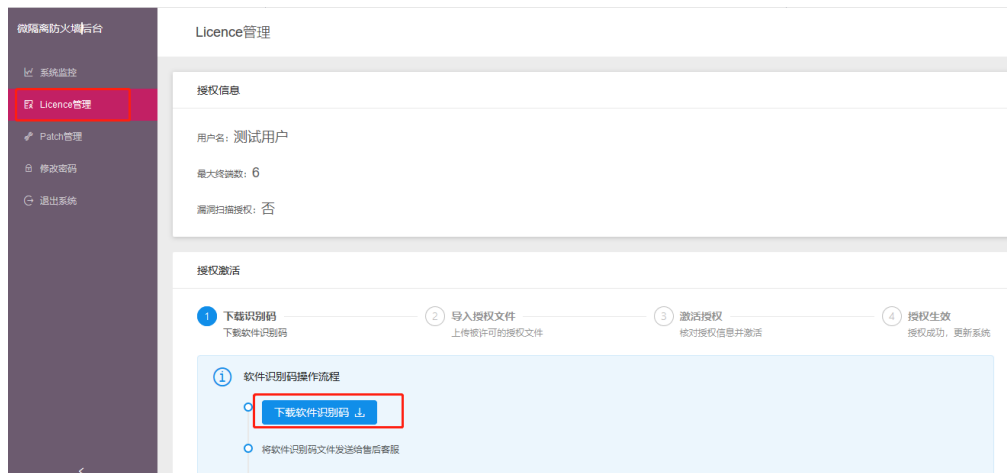


3.2 管理中心（QCC）授权

授权过程需要在后台管理页面进行。

3.2.1 导出识别文件

点击左侧导航栏的【License 管理】，在授权激活页面点击下载软件识别码。

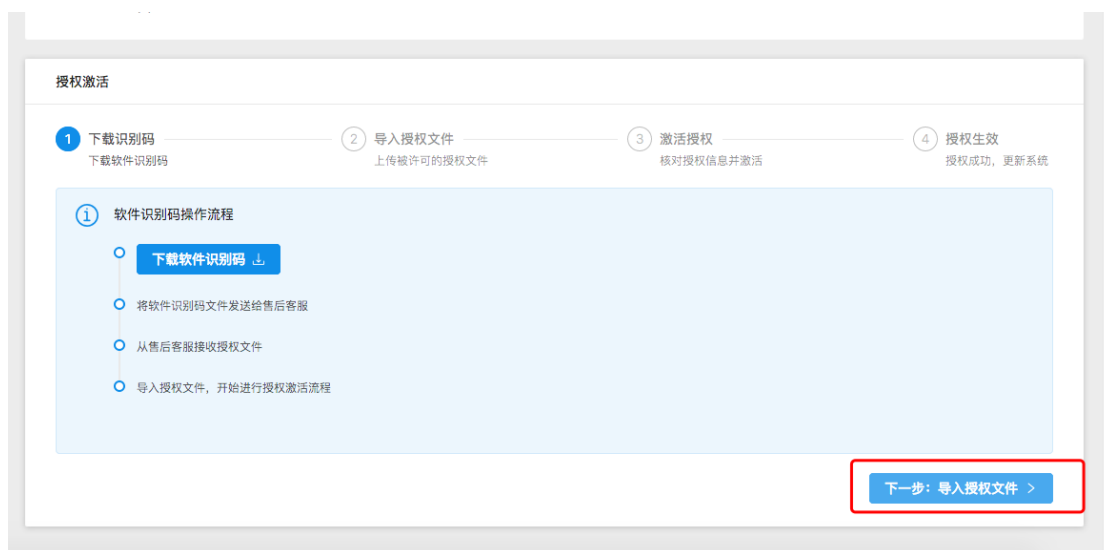


3.2.2 获取授权文件

将所下载的软件识别码发送给售后服务人员，售后服务人员将根据服务订单信息制作授权文件。制作好的授权文件将可通过邮箱、邮寄或其他方式传递给用户。

3.2.3 导入授权文件

收到授权文件后选择“导入授权文件”，并拖动相关授权文件进行上传，上传成功后进行“用户名”、“最大终端数”、“漏洞扫描授权”、“过期时间”等信息，确定无误后进行授权激活。



用户名: 测试用户

最大终端数: 6

漏洞扫描授权: 否

授权激活

1 下载识别码
下载软件识别码

2 导入授权文件
上传被许可的授权文件

3 激活授权
核对授权信息并激活

4 授权生效
授权成功, 更新系统

点击或拖动文件上传

< 上一步

用户名: 测试用户

最大终端数: 6

漏洞扫描授权: 否

授权激活

1 下载识别码
下载软件识别码

2 导入授权文件
上传被许可的授权文件

3 激活授权
核对授权信息并激活

4 授权生效
授权成功, 更新系统

核对授权信息

用户名: sjtest	最大终端数: 10	漏洞扫描授权: 是	过期时间: 2019-07-28 18:46:50
--------------------	------------------	------------------	----------------------------------

< 上一步

确定激活

授权信息

用户名: 测试用户

最大终端数: 6

漏洞扫描授权: 否

授权激活

1 下载识别码
下载软件识别码

2 导入授权文件
上传被许可的授权文件

3 激活授权
核对授权信息并激活

4 授权生效
授权成功, 更新系统

正在激活中。。。 58%

用户名: sjtest	最大终端数: 10	漏洞扫描授权: 是	过期时间: 2019-07-28 18:46:50
--------------------	------------------	------------------	----------------------------------

授权成功后可在 Licence 管理中查看系统授权信息。

Licence管理

授权信息

用户名: 测试用户

最大终端数: 6


漏洞扫描授权: 否

3. 3可视化分析使用说明

3.3.1 首界面/业务拓扑基本功能说明

1. 为了更好的展示及说明业务拓扑的功能及操作，以下使用已包含多台工作负载的微隔离防火墙进行说明。Demo 界面如下：




2. 页面左上角的  标识，点击后会弹出平台功能列表，如下图所示，点击各功能标签可进入各功能页面。

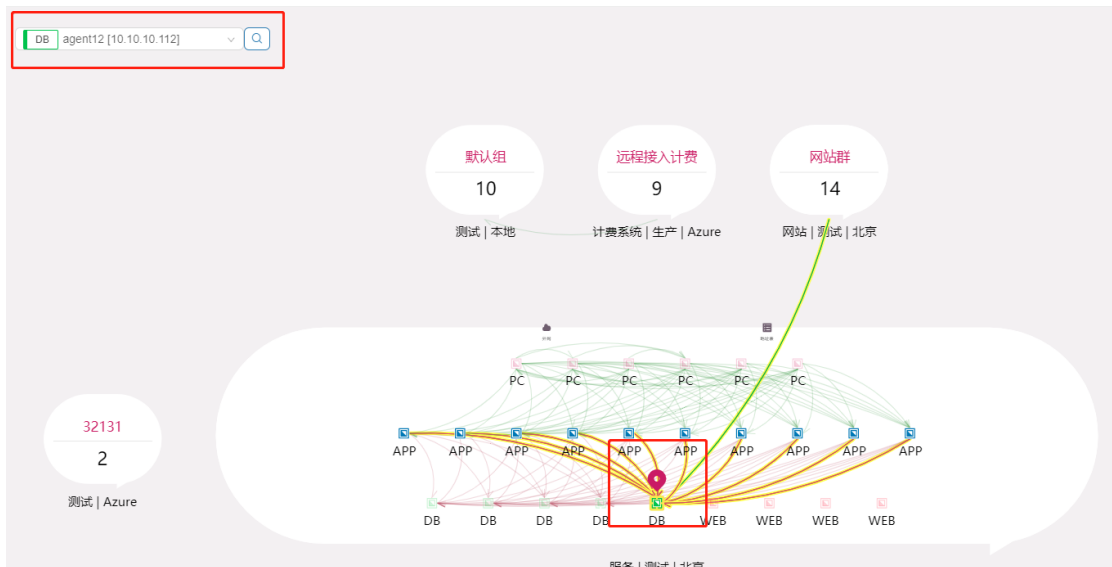


3. 页面上部的搜索框可对业务拓扑页面的工作组进行筛选。支持按工作组名称及工作组标签进行筛选。





4. 拓扑图左上角第二个搜索框为工作负载搜索框，支持 IP、主机名、角色标签匹配，选

择某工作负载后点击 ，即可在拓扑图中高亮显示此工作负载。如图所示。




5. 点击页面右侧的 **虚拟中心：默认** ，可以切换当前用户的其他虚拟中心。


6. 界面右侧的  标志，为发布提示标志，当平台的某些操作会影响安全策略时，

该图标会显示操作的数量 。点击该图标可进入发布审阅界面，确认发布后，此次操作造成的策略变动会同步到工作负载上。




发布状态	对象类型	名称	显示名称	最后修改人	修改时间
新添加	策略	yizhuangceshi	测试策略集	admin	2018-08-03 13:14:16
新添加	范围	yizhuangceshi		admin	2018-08-03 13:14:16
新添加	工作组	testgroup2	测试组	admin	2018-08-03 13:06:39
新添加	工作组	testgroup3	测试组	admin	2018-08-03 13:05:45
	规则	dockertest		admin	2018-08-03 13:05:45
	规则	dockertest		admin	2018-08-03 13:05:35

7. 首界面拓扑右上角的图例  标志，点击后可查看业务拓扑界面元素说明。



8. 图例标识右侧的过滤  标识，点击后，可对拓扑中的连接线及工作负载进行过滤，如下图所示：



9. 最右侧的  标识可对界面进行全屏展示， 以及  标识可以放大或缩小拓扑。

10. 右下角为“鹰眼”图标，拖动“鹰眼”中的灰框可以改变拓扑的位置，便于在工作组

较多时快速查看。



3.3.2 业务拓扑使用说明

1. 工作组

-拓扑中每个椭圆形标识代表一个工作组，类似于传统安全中的安全域、业务组等概念。

-每个工作组有 1-3 个标签，分为位置标签、应用标签、环境标签，可以通过这三个标签来标识一个工作组，例如：“北京|电商|生产”、“阿里云|web|测试”等。

-单击工作组，可查看该组的基本信息。基本信息页面可以修改该工作组的标签及策略状态。



工作负载	数量
APP	10
PC	6
DB	5
WEB	4

业务分组: 服务 | 测试 | 北京

策略状态: 测试

大数据

25

服务 | 测试 | 北京

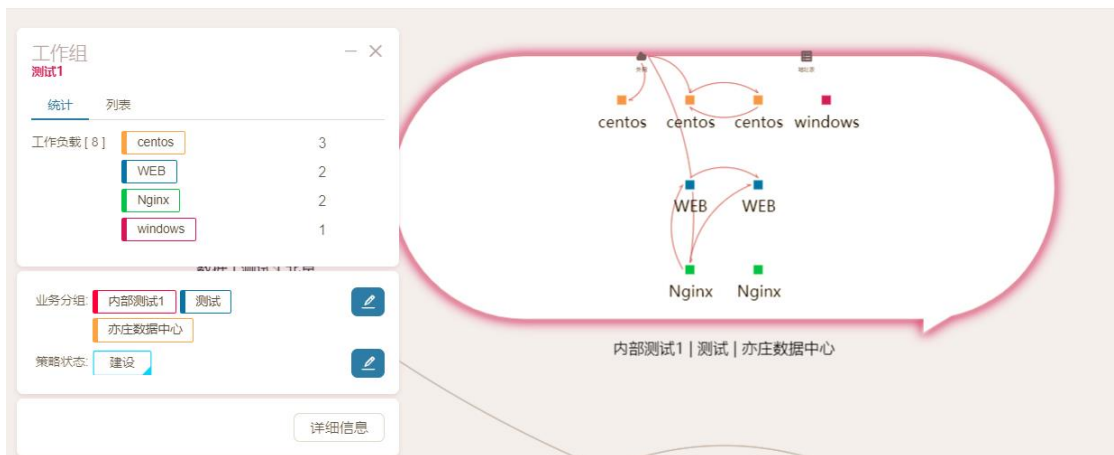
注意: 1. 标签的修改会导致策略的变化，在防护状态下，谨慎修改。

2. 针对工作组修改策略状态时，会改变改组内所有工作负载的策略状态。

-点击详细信息，可进入工作组的详细页面。



-双击工作组，可展开此工作组，并查看其中工作负载。



2. 工作负载

-工作组中每个小方块代表一个工作负载（工作负载可以是物理服务器、虚拟机或容器）。

-单击工作负载，可查看该工作负载的基本信息，拓扑中也会高亮显示与此工作负载有访问关系的其他工作负载。



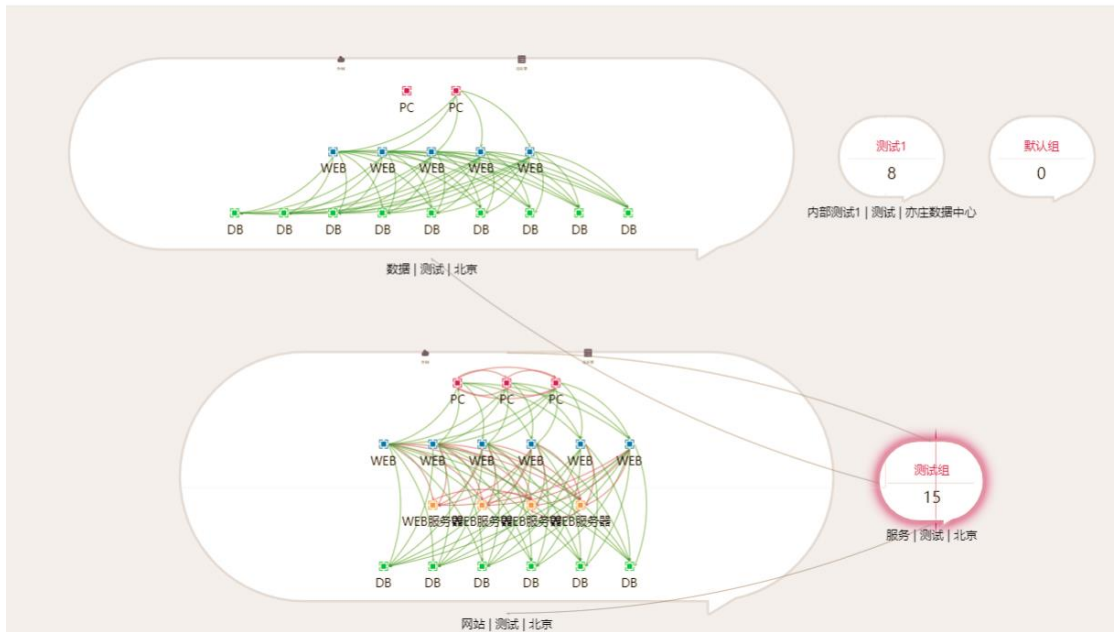
-在工作负载基本信息框中可快速修改该工作负载角色及策略状态。重新统计按钮可清空所有针对此工作负载的访问连接记录。

-支持在基本信息框中直接新建角色。



3. 连接线

-拓扑中每条连接线均代表此元素对于工作负载的访问连接，拓扑中的元素包括外网、地址表、工作负载。



-单击连接线，可查看该元素与此工作负载的所有连接情况，包括服务、端口、次数等信息。

业务流量

centos7 ← 外网

服务[2]

Sshd [tcp/22]	2932
Nginx [tcp/80]	183

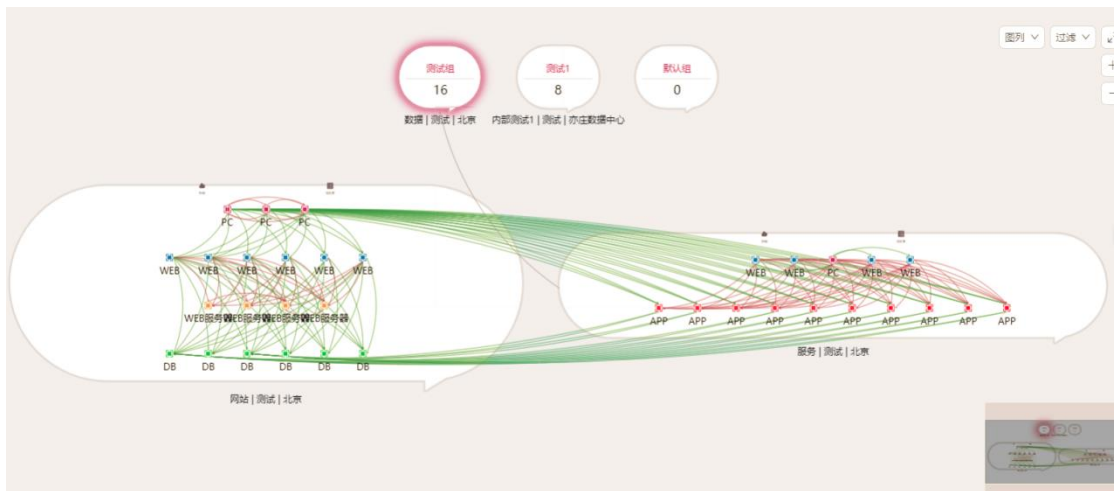
首次访问时间: 2017-10-23 10:22:35
最新访问时间: 2017-10-25 11:24:38

服务提供者: centos7

服务访问地址 [161]

101.230.198.136	103.27.238.213	104.131.124.154
106.120.40.28	106.39.39.18	106.39.39.28
106.75.63.218	109.195.86.75	109.195.94.50
111.127.118.22	111.40.120.33	113.113.120.243
113.05.40.150	114.44.420.52	114.248.108.442

-单击组间连线，可展开连线两端的工作组，并查看两组间的所有组间访问。



-红色连线说明此条连线中存在不合规的访问，绿色线为两元素之间的访问均符合规则。

-单击某条连线，还可直接查看或添加安全策略。

业务流量
agent42 ← agent23

服务[1]
Mysql [tcp/3306] 8
最新访问时间: 2018-10-11 15:39:36
服务提供者: agent42 DB
服务访问者: agent23 APP

重新统计 添加策略 ^

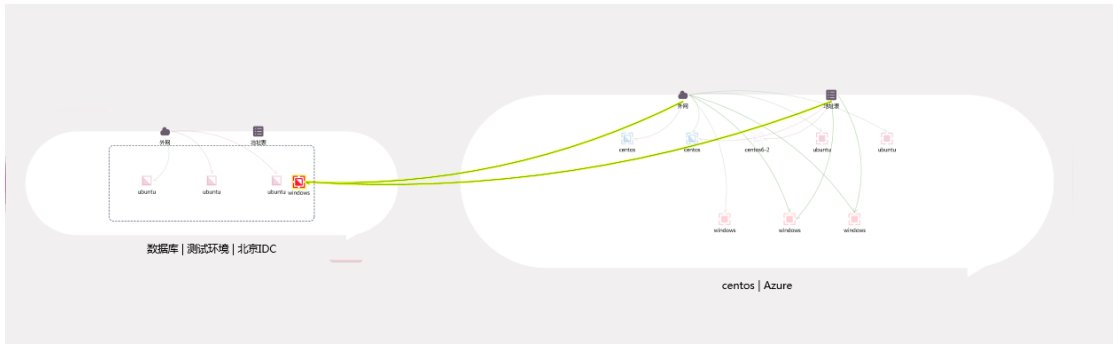
策略集: 1234 ×
服务: Mysql ×
提供者: 角色: DB ×
访问者: 角色: APP ×

新建

4. 元素拖动

-工作负载以及工作组均可进行拖动，以便根据业务需求调整拓扑。

-工作负载移动到其他工作组时，自适应引擎会自动计算并将新工作组的安全策略动态的加载到该工作负载。

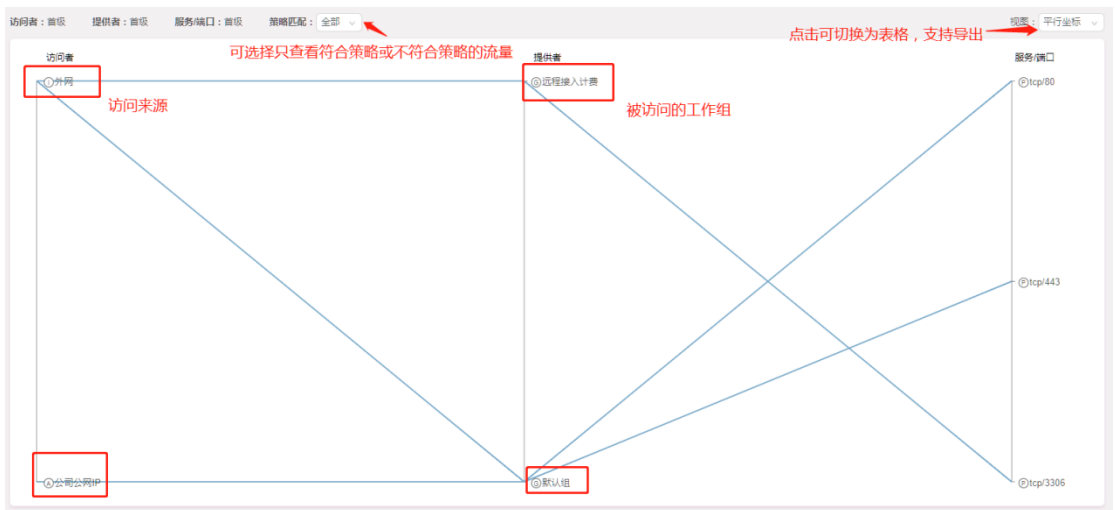


3.3.3 连接分析使用说明

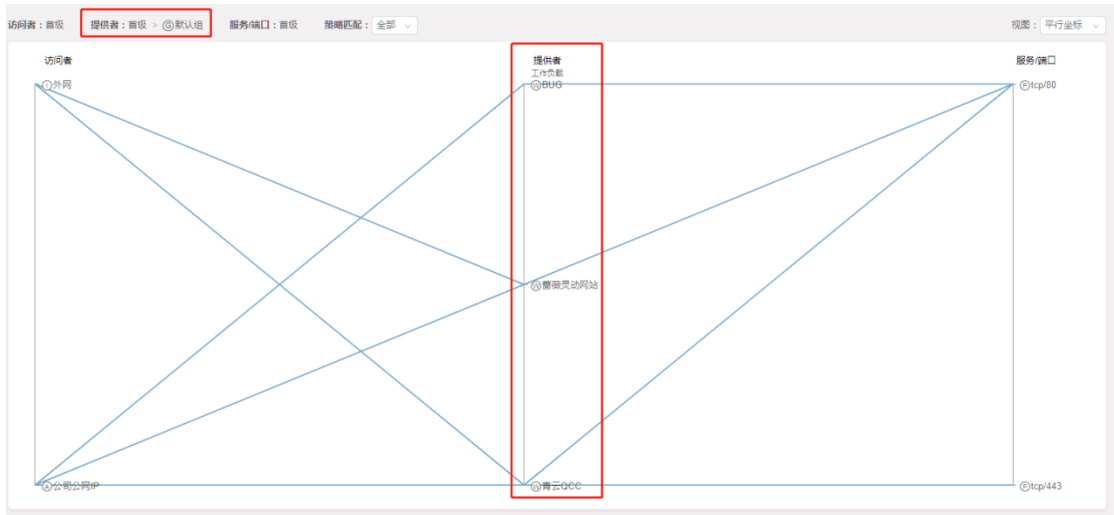
1. 点击菜单栏-连接分析，可进入连接分析界面。连接分析页面可帮助用户对于内部流量有针对性的进行筛选、钻取、分析。
2. 按照提示，选择访问者、服务提供者，选择想要查看、分析的对应服务、端口（可添加多个服务），次数以及时间周期。如图所示。



3. 添加好相应条件后，点击 **查询**，即可根据查看如下界面。



4. 如果访问者、提供者工作组时，还可点击此工作组，进一步对信息进行钻取，如下图所示。

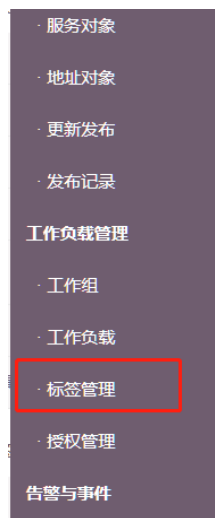


3.4 创建工作组

在接入工作负载之前，推荐先根据业务情况创建工作组，以便于后续工作负载直接接入对应的工作组（也可以先预设几个组，接入工作负载后，再根据业务进行组的划分）。

3.4.1 新建组标签

1. 首先点击菜单栏的标签管理：



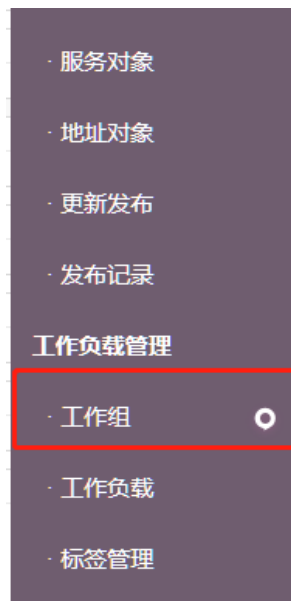
2. 进入标签管理页面后，根据业务属性，创建对应的位置、环境、应用标签（用于后续定义工作组）。

 标签管理


3. 标签分为名称及显示名称，名称支持英文、数字及下划线组合，且唯一。显示名称可以为中文，不唯一。

3.4.2 创建工作组

1. 点击菜单栏的工作组，进入工作组管理页面：



2. 点击新建，在弹出的对话框中输入此工作组的相关信息，根据业务情况选择事先创建的标签。每个工作组由 0-3 个组标签定义，若某一项无标签，可不选择。

注：当工作组无标签时，无法匹配策略。

新建工作组

* 名称: 支持中文、英文、数字及下划线组合

* 显示名称: 输入标签的显示名称, 可以支持中文字符

地点: 选择或筛选位置标签

应用: 选择或筛选应用标签

环境: 选择或筛选环境标签

描述: 输入描述, 可以支持中文字符

取消 确定

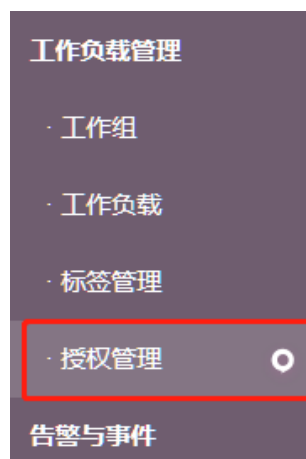
3. 点击确定后, 工作组建立完成, 拓扑图中会出现该工作组。

3.5 接入工作负载 (BEA 端)

3.5.1 创建授权码

说明: 授权码代表了工作负载的身份, 一个工作负载在接入系统时, 系统将根据其授权码决定是否允许其接入、配置什么样的安全策略、分配到哪个工作组等。

1. 创建授权码有两个入口, 一个是菜单栏的授权管理, 通过此入口可以查看管理所有授权码。

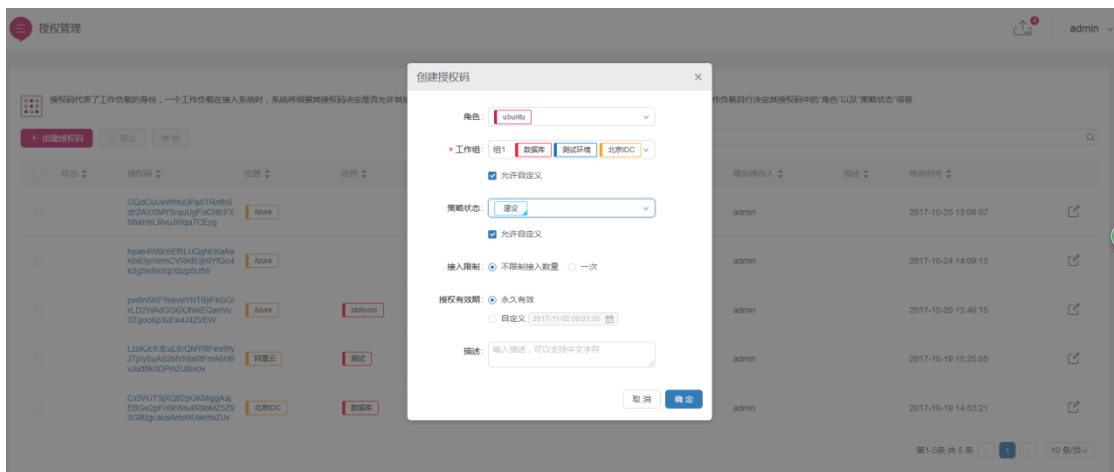


第二个入口, 可以通过工作组详情查看该工作组的授权码 (由某个组的授权码接入的工作负载, 将自动分配到该工作组)。



2. 创建授权码

点击创建授权码，在弹出的对话框中输入相关参数。点击确定即可完成授权码的建立。



2. 点击授权码，可进入授权码详细页面。



3. 授权码详细页面最下方的自动化安装部分，可根据此授权码自动生成安装命令，用于实现工作负载的自动化安装。

The screenshot shows a configuration interface for an authorization code. At the top, there are tabs for '允许自定义' (Allow Customization), '测试' (Test), '私有云' (Private Cloud), and 'web1'. Below this, there are sections for '策略状态' (Policy Status) with '不允许自定义' (Do not allow customization) selected and a '建设' (Construction) button, '接入限制' (Access Limit) set to '无限制' (No limit), and '有效期' (Validity Period) set to '永久' (Forever). The '自动化安装' (Automation Installation) section is highlighted with a red box and contains a dropdown menu set to 'Centos / 7 x'. Below the dropdown is a text area containing a long command: `sudo curl http://.../bea.sh -o /tmp/bea.sh && sudo chmod +x /tmp/bea.sh && sudo /tmp/bea.sh -m ... -a ...`. A '复制安装命令' (Copy Installation Command) button is located at the bottom right of the text area.

注意：1. 执行该命令，系统会自动到管理中心下载安装脚本，请确保安装客户端的工作负载与管理中心网络可达。

2. 安装脚本执行后自动判定系统版本，并从管理中心获取相应安装包。

3. linux 系统安装命令一致、Windows 系统安装命令一致。

4. agent 成功安装后，不会清空原有 iptables 中的策略。后续产品添加安全策略会在 iptables 最上层添加。若只在监测模式下运行，可在安装命令后加 `-nf true` 则不安装产品防护模块。

3.5.2 接入工作负载

-复制生成的安装命令，linux 系统用 root 用户远程登录后执行该命令。

-Windows Server 可在 cmd（管理员权限下）中执行。

-也可以使用自动化运维工具进行批量安装。

注意：1. ubuntu 在 14.04 之后的版本不支持 root 用户登录，可使用具备 root 权限的用户登录后执行。

2. 由于系统可能进行了各类安全设置，例如不允许在 root 下执行 sudo，不允许安装软件，不允许运行脚本，安装源不允许修改等，如遇到安装不成功时，可联系我方工程师进行协助。

3. 如不需要安装产品的防护模块，需在安装命令末尾输入 `-nf true`

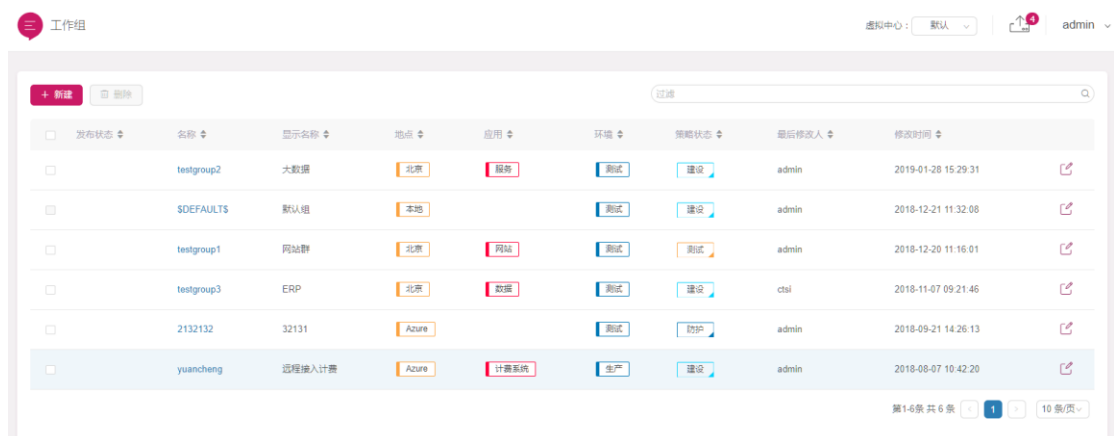
3.6 工作负载管理模块


工作负载管理模块包含三个部分：工作组、工作负载、标签管理、授权管理



3.6.1 工作组

1. 工作组，类似于传统安全中的安全域、业务组等概念。每个工作组有 1-3 个标签，分为位置标签、应用标签、环境标签，可以通过这三个标签来标识一个工作组，例如：“北京|电商|生产”、“阿里云|web|测试”等。工作组页面可以进行新建、修改、删除操作。



2. 工作组页面右上方的搜索框可以对工作组进行过滤，页面中基本属性栏可以进行排序， 下箭头为正序，上箭头为反序。

工作组 admin

[+ 新建](#) [- 删除](#)

发布状态	名称	显示名称	位置标签	应用标签	环境标签	策略状态	最后修改人	修改时间
<input type="checkbox"/>	test1	组1	北京IDC	数据库	测试环境	建设	admin	2017-10-25 15:05:38
<input type="checkbox"/>	test3	组3	Azure		centos	测试	admin	2017-10-25 14:46:56
<input type="checkbox"/>	idotoors	idotoors	Azure	idotoors	idotoors	建设	admin	2017-10-20 05:46:06
<input type="checkbox"/>	test4	组4	阿里云	测试	centos	建设	admin	2017-10-19 07:24:56
<input type="checkbox"/>	\$DEFAULT\$	默认组				建设	admin	2017-10-19 06:34:44

第1-5条 共5条 1 10条/页

+ 新建

3. 点击 **+ 新建** 按钮，即可在弹出框中进行工作组的建立，一个工作组名称唯一，并选择 1-3 个标签。新建的工作组会出现在业务拓扑页面。

4. 点击工作组名称可进入工作组详细页面。详细页面分为基础信息、工作负载、策略、授权管理、包管理。

工作组 > 组1

[基础信息](#) [工作负载](#) [策略](#) [授权管理](#) [包管理](#)

概要信息

名称	test1
显示名称	组1
描述	
发布状态	
策略状态	建设
最后修改人	admin
最后修改时间	2017-10-25 15:05:38

标签信息

应用标签	数据库	环境标签	测试环境	位置标签	北京IDC
------	-----	------	------	------	-------

5. 工作负载详情页面中的工作负载页面，可查看当前此工作组包含哪些工作负载，在此页面可批量将工作负载调整到外部，也可选择其他组的工作负载调整到本组。



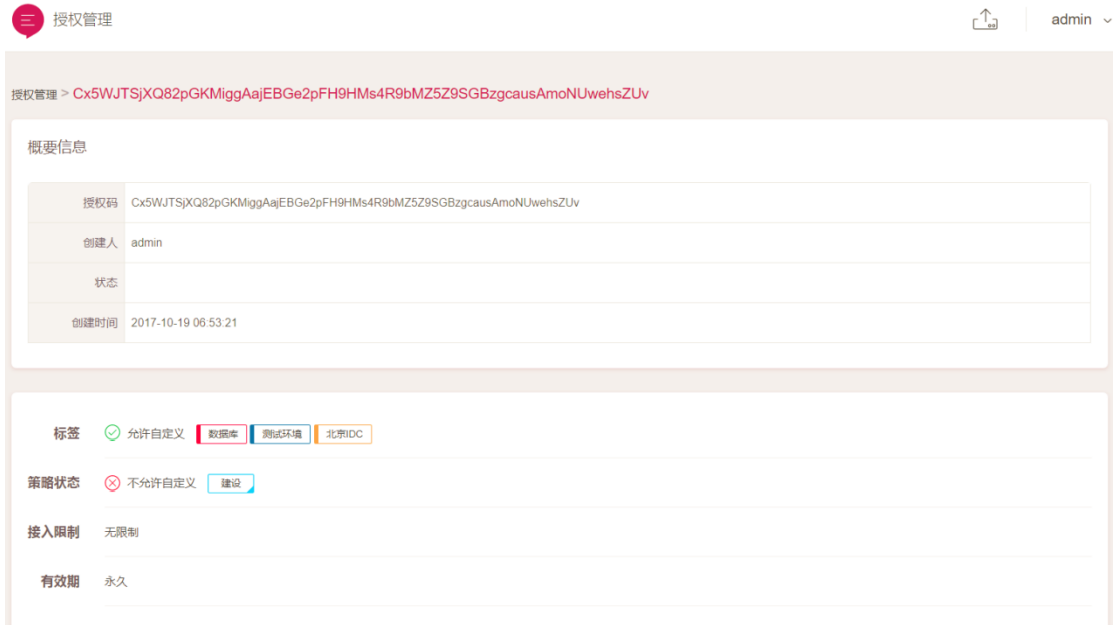
6. 工作组详情页面中的策略页面，可查看作用于该工作组的所有策略，并可以调整本组的策略状态。点击展开可查看策略详情。



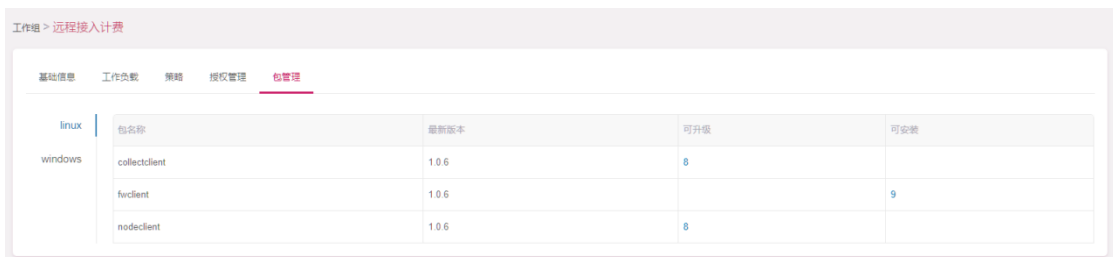
7. 工作负载详情页面中的策略页面，可查看与本工作组相关的授权码，即通过本授权码安装的工作负载，均自动位于该工作组。



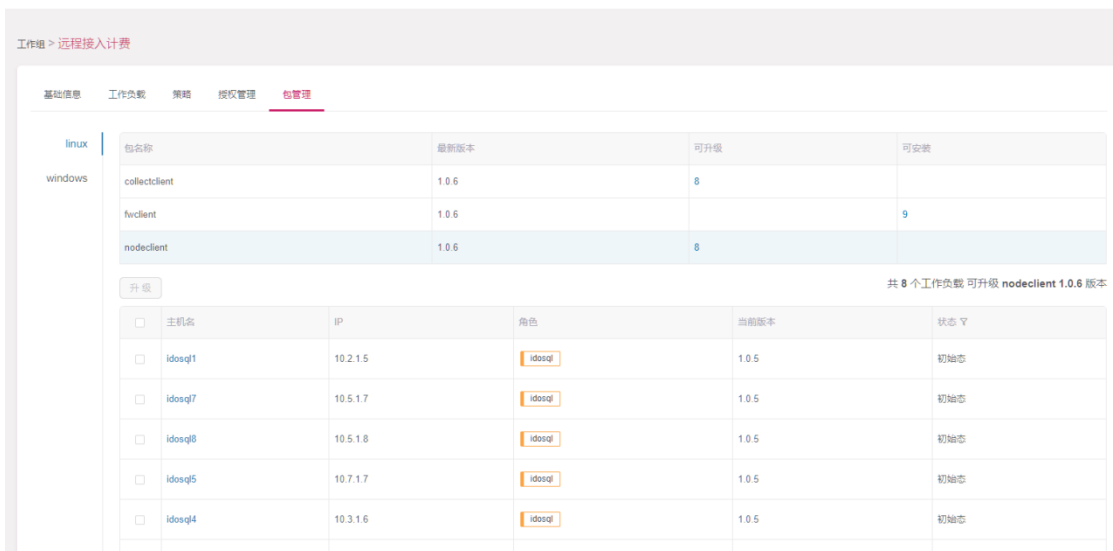
8. 点击授权码，可进入授权码详情页面。



9. 工作负载详情页面中的包管理页面，包管理页面用于客户端模块的安装和升级，包含本组所有工作负载。



10. 点击其中显示的数字，可显示具体工作负载 Agent 的版本信息。



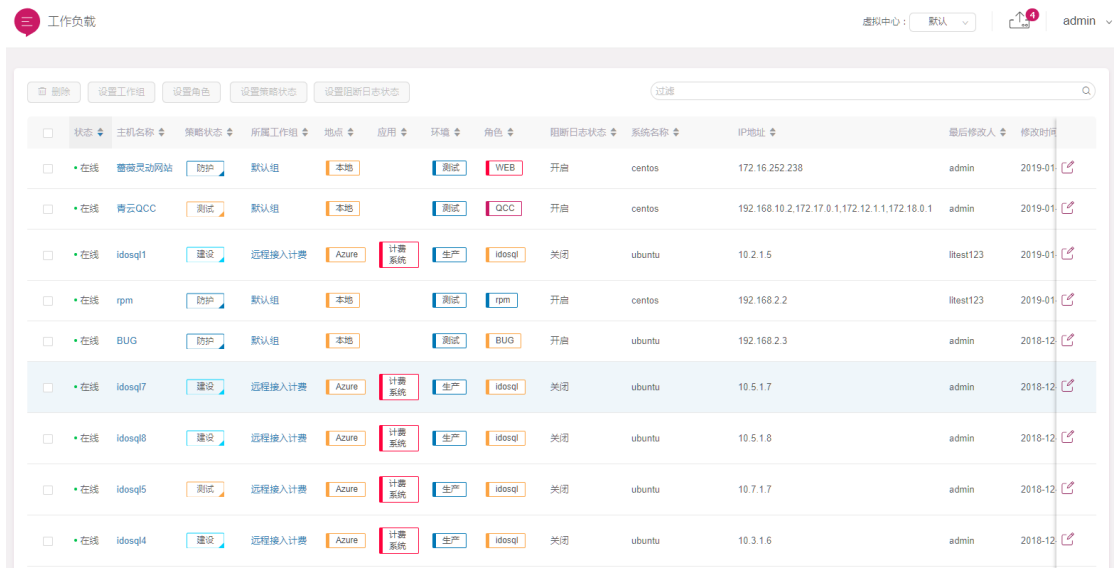
3.6.2 工作负载

1. 点击工作负载即可进入工作负载列表。

-工作负载列表可以对所有的工作负载进行查看，并可以借助排序、搜索等方式对工作负

载进行过滤。

-同时此页面还支持对工作负载进行批量的修改及删除。



2. 点击工作负载的主机名称，可进入该工作负载的详细信息页面，包括其基本信息、服务信息、策略信息、阻断日志及相似计算。

-服务信息：可查看此工作负载所有有网络监听的服务，以及对应的端口、进程。

-策略：可查看此工作负载目前所生效的安全策略。

-阻断信息：如果开启阻断日志、且工作负载处于测试或防护状态，即可查看阻断日志的。

-相似计算：根据工作负载的基本信息、所开放的服务端口以及连接等信息，计算其他工作负载与此工作负载的相似程度。便于对业务进行分析。



3.6.3 标签管理

标签用于描述工作组的相关属性以及工作负载的具体角色。

-组标签分为三类：位置，应用，环境。

-可以根据需要创建、删除或修改不同类型的标签。

-标签分为名称及显示名称，名称必须为英文及数字的组合，且唯一。显示名称可以为中文，不唯一。

注意：当要删除角色标签时，此角色标签需未被赋予任何工作负载。工作组标签删除时同理。

3.7 安全策略管理模块


安全策略管理模块包括策略与策略集、服务对象、地址对象、更新发布、发布记录。服务对象、地址对象子模块主要为策略与策略集的建立提供支撑。更新发布、发布记录用于策略的发布流程以及后续查看、回滚。

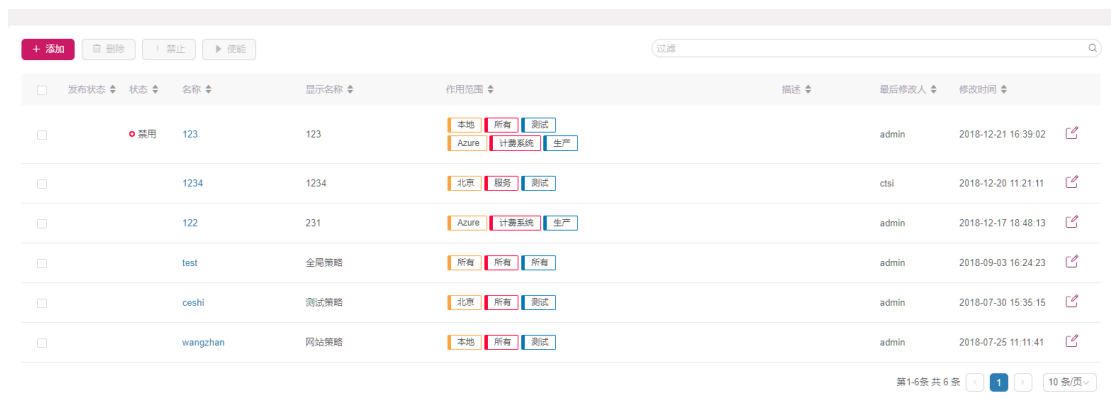
注意：1. 建议用户为每一个工作组建立一个策略集，便于后续的运维。

2. 全局策略在命名时要标识出是全局策略，便于后续运维。

3.7.1 策略与策略集

1. 策略与策略集用于策略的建立、修改、删除、禁止与使能。可通过页面的搜索框进行

过滤；每条策略最右侧的  图标用于修改该条策略的基本信息。界面如下：

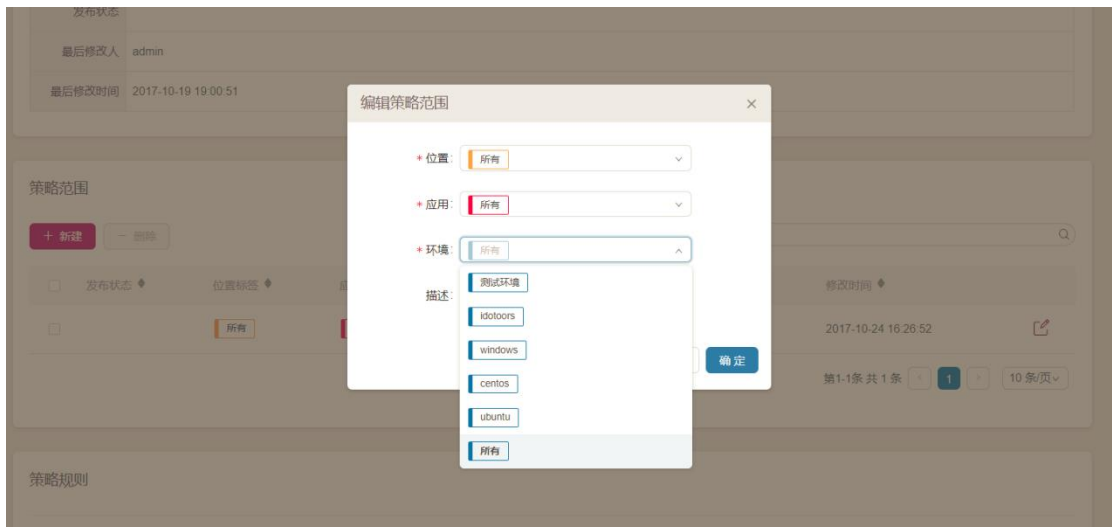


发布状态	状态	名称	显示名称	作用范围	描述	最后修改人	修改时间
<input type="checkbox"/>	禁用	123	123	本地 所有 测试 Azure 计费系统 生产		admin	2018-12-21 16:39:02
<input type="checkbox"/>		1234	1234	北京 服务 测试		ctsi	2018-12-20 11:21:11
<input type="checkbox"/>		122	231	Azure 计费系统 生产		admin	2018-12-17 18:48:13
<input type="checkbox"/>		test	全局策略	所有 所有 所有		admin	2018-09-03 16:24:23
<input type="checkbox"/>		ceshi	测试策略	北京 所有 测试		admin	2018-07-30 15:35:15
<input type="checkbox"/>		wangzhan	网站策略	本地 所有 测试		admin	2018-07-25 11:11:41

2. 点击添加，在弹出框内输入名称等信息，即可新建一条策略。

3. 新建策略后，点击策略名称，可进入策略详细页面，详细页面可查看该策略的详细信息，并可配置策略的作用范围，策略的详细规则，策略分为范围内策略与范围外策略。

4. 策略范围是通过选择工作组标签来设定的，若策略范围所选定的标签涵盖某工作组的标签，则该策略集对此工作组生效。




5. 策略规则分为范围内规则和范围外规则，分为作用于策略范围所涵盖的工作组内和范围外对该范围内的访问规则。

-在范围内规则处点击新建，弹出框中设置本条规则的服务提供者，所提供的服务，以及允许的访问者。

例如，我们让标签为 DB 的工作负载可以访问标签为 APP 的工作负载的 Mysql (tcp/3306) 服务，具体设置如下图：



注意：1. 可在新建规则时，直接新建标签及服务。2. 可以选择某一个工作负载。

6. 对于已建立的规则可以点击每条规则最右侧的  标志进行修改。服务者和访问者均可多选，而服务只能单项选择。

7. 工作组间规则的设置如上，其作用于范围外对范围内的访问。

3.7.2 服务对象


1. 服务对象是指用户已知允许访问的服务，描述一个服务对象需要包含服务名称、传输协议（tcp/udp）、服务所要使用的端口范围。

windowstest	端口范围测试	tcp/3380-3389,udp/3380-3389
-------------	--------	-----------------------------

2. 服务对象页面可以建立、修改、删除服务，上方的搜索框可以根据输入对服务对象进行过滤。



状态	名称	显示名称	服务	描述	最后修改人	修改时间
<input type="checkbox"/>	Mysqld		tcp/3306		admin	2017-10-26 07:18:53
<input type="checkbox"/>	Nginx		tcp/80		admin	2017-10-25 09:39:15
<input type="checkbox"/>	MyWebServer.exe		tcp/10080		admin	2017-10-24 09:38:45
<input type="checkbox"/>	svchost.exe		tcp/3389		admin	2017-10-24 09:37:47
<input type="checkbox"/>	unkown	test2	tcp/80-89		admin	2017-10-20 10:05:34
<input type="checkbox"/>	windowstest	端口范围测试	tcp/3380-3389,udp/3380-3389		admin	2017-10-20 06:51:28
<input type="checkbox"/>	ssh	ssh	tcp/22		admin	2017-10-19 11:00:39

3. 点击  按钮，可以建立一条新的服务，服务名称不可相同，需要注意协议和端口的书写要求，端口可以用范围表示，多个协议和端口可用逗号隔开。

创建服务


* 名称: 输入名称, 仅支持大小写英文字符

* 显示名称: 输入显示名称, 可以支持中文字符

* 服务 [?]: 按照 协议/端口的格式书写, 以逗号分隔
例如:
tcp/80-88,udp/45

描述: 输入描述, 可以支持中文字符

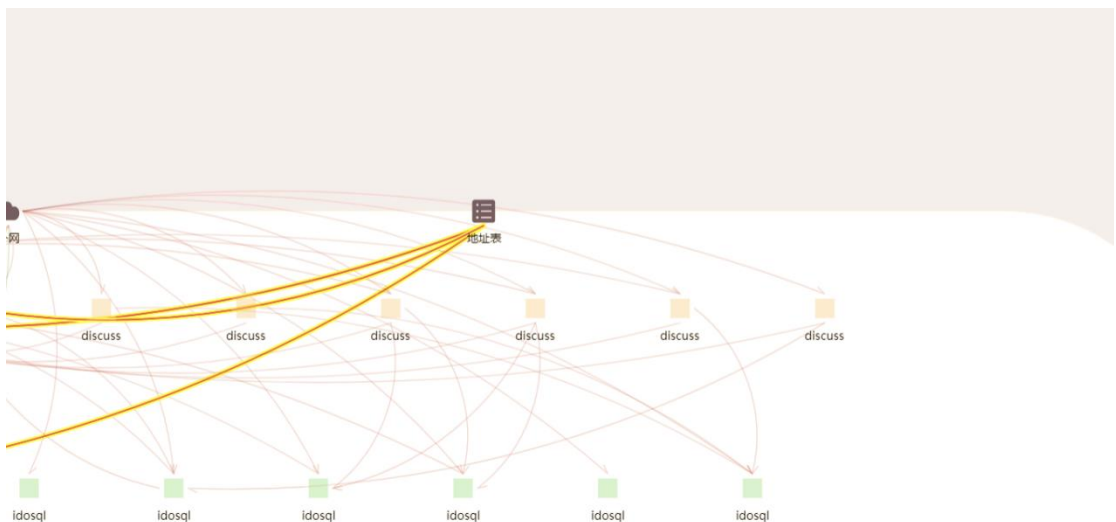
取消 确定

4. 点击每条服务对象最右侧的  标识可对服务对象进行修改, 名称不可修改。可修改显示名称及服务的协议端口。



3.7.3 地址对象

1. 地址对象是指某些我们已知的 IP 地址，这些 IP 地址配置成地址对象后，便于策略的建立，并且在业务拓扑图中来自地址对象的 IP 连接会转移到地址表中进行显示。如下图所示：



2. 地址对象页面可以对地址对象进行新建、删除、修改操作。



+ 新建

3. 点击 **+ 新建** 标识，可新建一条地址对象。地址对象名称唯一，需注意地址的书写格式，IP 段用 IP 地址加掩码表示，如果为单个 IP 地址也需标注 32 位掩码，多个地址中间用逗号隔开。

4. 点击每条地址对象最右侧的  标识，可对地址对象进行修改。



- 删除

5. 勾选对应的地址对象，点击 **- 删除** 按钮，可进行删除操作。

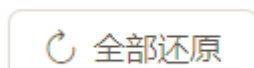
地址对象

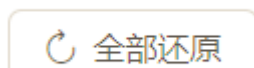


3.7.4 更新发布

1. 更新发布有两个作用，一是可以记录本次需要发布的所有操作，便于审阅；二是通过本页面点击发布，将本次的所有操作同步到 Agent。



 全部还原

2. 点击  按钮，可将本次还未发布的操作进行还原。

3.7.5 发布记录

1. 发布记录页面会记录每次发布的内容，包括分发状态，描述，发布人，发布时间等信

息。

发布记录 admin

ID	发布状态	描述	最后修改人	修改时间	与当前配置比较
59f18c915607c0000117739b	分发完成	qqq	admin	2017-10-26 07:19:45	与当前配置比较
59ef24b15607c00001177395	分发完成	uuu	admin	2017-10-24 11:32:01	与当前配置比较
59eefa515607c0000117738f	分发完成	ww	admin	2017-10-24 08:31:13	与当前配置比较
59eef9b5607c0000117738d	分发完成	qqq	admin	2017-10-24 08:29:47	与当前配置比较
59e9ca8a5607c0000117738c	分发完成	kk	admin	2017-10-20 10:06:02	与当前配置比较
59e9c8f45607c0000117738b	分发完成	就	admin	2017-10-20 09:59:16	与当前配置比较
59e9c88f5607c0000117738a	分发完成	人	admin	2017-10-20 09:57:35	与当前配置比较
59e9c3f05607c00001177389	分发完成	hh	admin	2017-10-20 09:37:52	与当前配置比较

与当前配置比较

2. 点击每条发布记录最右侧的 [与当前配置比较](#)，即可进入比较页面，本页面会显示本条发布记录时与现有策略的差别项。

发布记录 admin

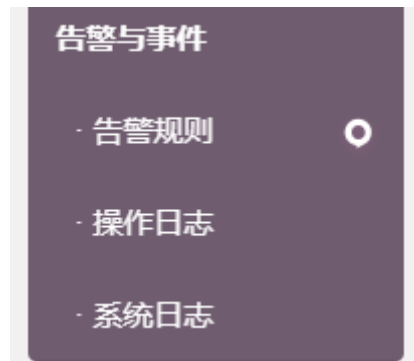
发布记录 > 59ef24b15607c00001177395

比较结果

发布状态	对象类型	名称	显示名称	最后修改人	修改时间
被修改	工作组	test1	组1	admin	2017-10-25 15:05:38
被修改	工作组	test3	组3	admin	2017-10-25 14:46:56
新添加	规则	test1		admin	2017-10-25 09:39:15
新添加	规则	test1		admin	2017-10-26 07:18:53
新添加	服务对象	Nginx		admin	2017-10-25 09:39:15
新添加	服务对象	Mysqld		admin	2017-10-26 07:18:53

3.8 告警与事件

点击菜单栏最下方告警与事件-系统操作日志，可进入系统操作日志界面。



3.8.1 告警规则

进入告警规则界面后，可配置告警相关信息（邮件服务器地址需 admin 用户在系统管理中设置）。根据下图步骤可完成告警规则的配置。



告警规则配置界面截图，包含以下配置项：

- 基本信息**：
 - 名称：1.名称会显示在邮件中，也便于后续管理
 - 告警类别：2.选择告警类别
- 告警行为**：
 - 告警周期：3.每次告警的时间间隔
 - 生效开始：00:00，生效结束：23:59，时区：UTC +8
 - 4.在此时间段内发生的事件进行告警
 - 通知列表：5.选择被通知者，可事先设置通知列表。
- 告警条件**：
 - 6.不同告警类别，可选的告警条件不同，可自由组合
 - 日志类别：请选择日志类别
 - 日志标号：请选择日志标号
 - 日志内容：请选择日志内容
 - 最低日志级别：信息
 - + 增加条件

注意：1. 每次告警只通知上次告警之后发生的符合条件的事件

2. 对于日志类的告警，条件中类别类别较多，可通过事先查看日志具体内容来熟悉各类别含义。

3.8.2 操作日志

操作日志会记录用户的操作（包括 Web 页面及 API），例如工作组的创建、策略的生成等等。用户可根据筛选条件查看对应的操作日志。



3.8.3 系统日志

系统日志界面会记录系统的运行信息以及工作负载状态信息。可用于查看系统运行状态，工作负载运行状态，策略是否生效等。



3.9 系统配置

3.9.1 系统管理

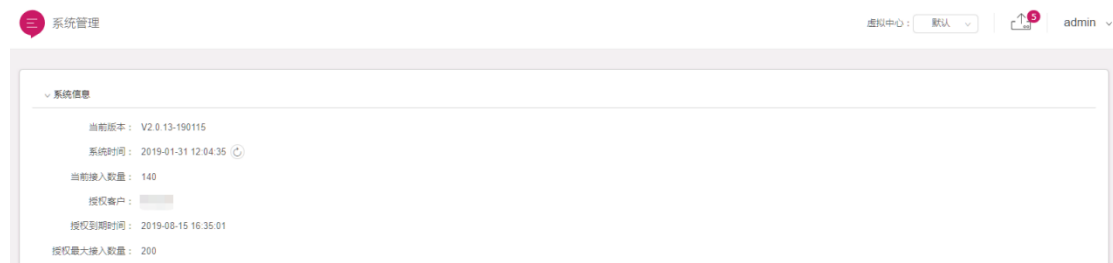
点击首界面右上角的用户名，即可进入系统管理，虚拟中心管理界面，账户管理，系统管理日志以及可退出当前用户。如下图所示：



系统管理可查看及设置系统相关参数，包括查看 license 相关参数、日志储存天数、登录尝试次数、会话时长，以及配置告警邮件发送服务器。

注意：只有超级管理员具备进入系统管理的权限。

系统信息：包含系统版本、系统时间、license 数量、授权时间、客户名称等信息。



注意：1) 当授权时间还有 1 周时会在页面上方进行提示。超过期限后，产品将禁止登录。

2) 已接入数量达到授权数量后，接入新工作负载将失败。

1. 系统设置：可设置系统日志、操作日志的储存天数。工作负载离线时间是指某一工作负载多久没有心跳时，管理中心认为其已经离线。
2. 登录设置：可设置各账户尝试登录次数，超过次数后账户锁定。还可会话时长设置中设置页面无操作时自动退出账户的时间。
3. 邮件发送服务器配置：若要配置邮件告警，需 admin 用户根据内部实际情况先配置邮件发送服务器地址。

告警邮件发送服务器设置

smtp地址: smtp.mxhchina.com

smtp端口: 465

发送邮件的地址: [redacted].com

发件人: 物联网平台

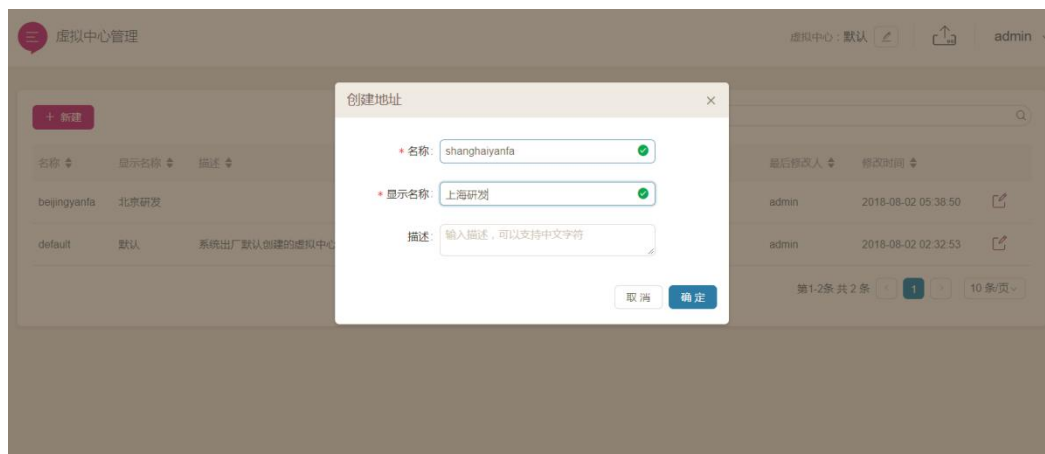
密码: [redacted]

重复密码: [redacted]

设置

3.9.2 虚拟中心管理

虚拟中心用于分租户/部门管理，建立不同虚拟中心后，创建用户时，可限定该用户可以访问的虚拟空间，该租户/部门下设的虚拟机接入到本用户的虚拟中心，只接受本租户/部门管理。



注意：admin 可以看到所有虚拟空间。

3.9.3 账户管理

1. 点击账户管理，即可进入账户管理页面，账户管理页面可查看用户登录信息，新增用户、修改密码等操作。

2. 账户分为超级管理员、管理员、审查员。

-超级管理员：默认为 admin，最高权限，可创建管理员及审查员。

-管理员：可以进行策略设置、工作组设置、工作负载接入等操作，但不能查看系统管理日志。

-审查员：只可以查看系统日志、操作日志及告警规则。

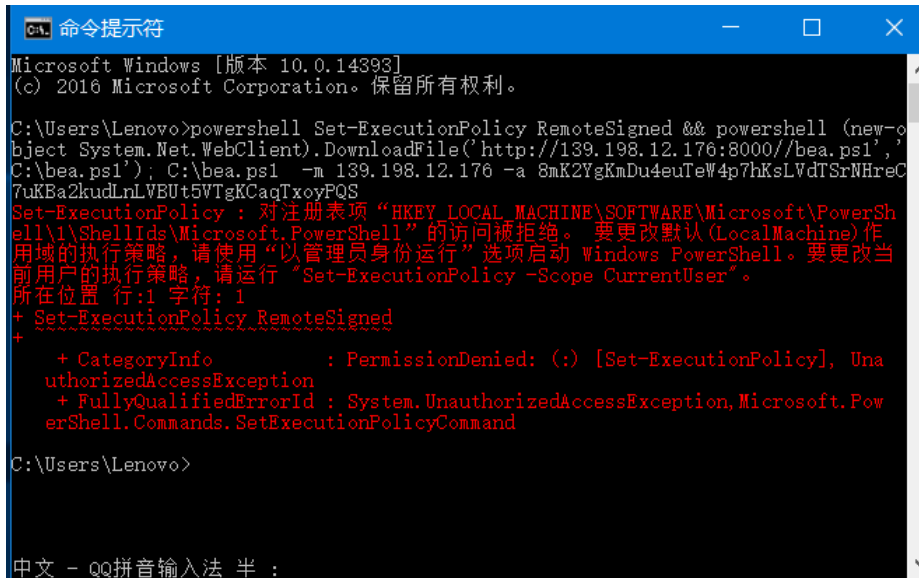


3. admin 可以在账户管理页面解锁被锁定的用户，也可针对某一用户生成 API 密钥。被生成 API 密钥的账户，可以使用 API 接口。



4 常见问题

Q: Windows 系统在安装客户端时，提示访问被拒绝，如下图所示：



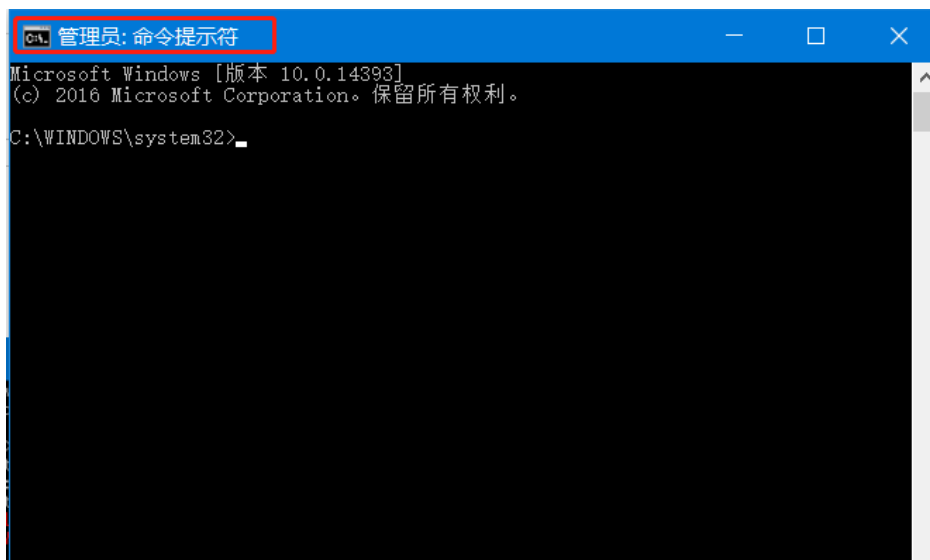
```

命令提示符
Microsoft Windows [版本 10.0.14393]
(c) 2016 Microsoft Corporation。保留所有权利。

C:\Users\Lenovo>powershell Set-ExecutionPolicy RemoteSigned && powershell (new-object System.Net.WebClient).DownloadFile('http://139.198.12.176:8000//bea.ps1', 'C:\bea.ps1'); C:\bea.ps1 -m 139.198.12.176 -a 8mK2YgKmDu4euTeV4p7hKsLVdTSrNHreC7uKBa2kudLnLWBUt5VTgKCaqTxoyPQS
Set-ExecutionPolicy : 对注册表项“HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\PowerShell\1\ShellIds\Microsoft.PowerShell”的访问被拒绝。要更改默认(LocalMachine)作用域的执行策略，请使用“以管理员身份运行”选项启动 Windows PowerShell。要更改当前用户的执行策略，请运行“Set-ExecutionPolicy -Scope CurrentUser”。
所在位置 行:1 字符: 1
+ Set-ExecutionPolicy RemoteSigned
+ ~~~~~
+ CategoryInfo          : PermissionDenied: (:) [Set-ExecutionPolicy], UnauthorizedAccessEx
+ FullyQualifiedErrorId : System.UnauthorizedAccessException,Microsoft.PowerShell.Commands.SetExecutionPolicyCommand

C:\Users\Lenovo>
    
```

A: 使用管理员权限运行 CMD，并执行安装命令。



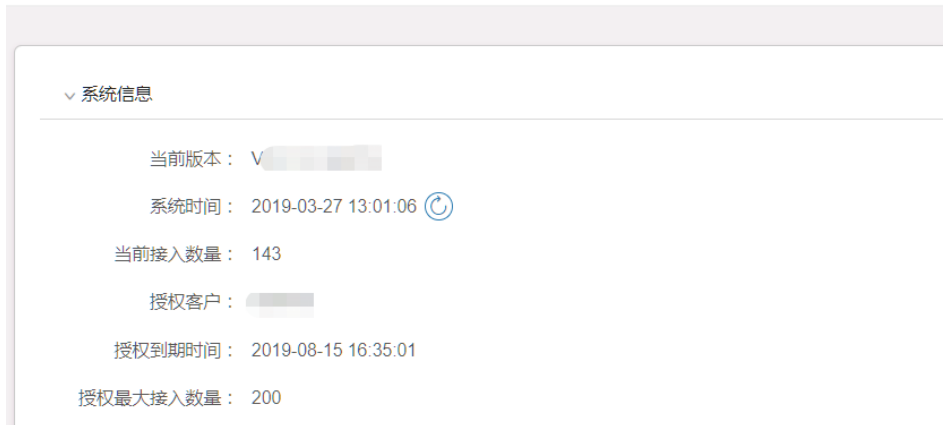
```

管理员: 命令提示符
Microsoft Windows [版本 10.0.14393]
(c) 2016 Microsoft Corporation。保留所有权利。


C:\WINDOWS\system32>
    
```

Q: 安装过程中无报错，但管理中心中未出现新安装的云主机

A: 查看 license 是否已到期或可接入数量已用满。

 系统管理

System Information

- 当前版本: V [redacted]
- 系统时间: 2019-03-27 13:01:06 
- 当前接入数量: 143
- 授权客户: [redacted]
- 授权到期时间: 2019-08-15 16:35:01
- 授权最大接入数量: 200

Q: 使用 IE 浏览器访问产品管理页面时，一直显示加载中

A: 目前产品不支持 IE 浏览器，可使用谷歌、火狐、Edge、腾讯、360 浏览器，推荐使用谷歌 Chrome 浏览器。

Q: 自适应微隔离产品需要对外提供那些端口访问，才能正常工作？

A: 需要提供如下端口 10443、6443、8000、60001、60011、60021、60031，其中 6443 为 WEB 控制台访问端口，8000 安装 agent 的访问端口，60001、600011、60021、60031 为 agent 接入自适应微隔离管理中心的使用端口，10443 端口为后台管理使用的端口。

Q: 自适应微隔离产品的管理控制台登录方式？

A: 自适应微隔离产品提供镜像模式，请访问基于此镜像启动云主机的 IP 地址，访问方式如下 <https://xxx.xxx.xxx.xxx>，访问请忽略证书安全性要求，继续访问即可。

Q: 自适应微隔离 WEB 控制台必需使用何种浏览器？

A: 自适应微隔离产品使用了现代浏览器的特性，推荐使用 chrome 73 以上版本、edge 17 以上版本或者 Safari 11 版本以上

Q: 自适应微隔离 WEB 控制台初始的登录用户名密码是什么？

A: 出厂的默认用户名: admin, 密码: admin@338

Q: 自适应微隔离 WEB 控制台密码被锁定了怎么办?

A: 系统默认设置为密码重试 4 次将被锁定，一种方法是重启安装本产品云主机，密码锁定被恢复。

Q: 自适应微隔离 web 控制台忘记登录密码怎么办?

A: 请联系客服人员进行密码重置

Q: 如何获取自适应微隔离的客户端安装命令?

A: WEB 端登录系统后，在 工作负载管理=>授权管理 中创建授权码，在页面下方可以获取针对不同的操作系统获取自动化安装命令，如下图



比如 Windows 安装命令如下:

```
powershell Set-ExecutionPolicy RemoteSigned && powershell (new-object
System.Net.WebClient).DownloadFile('http://xxx.xxx.xxx.xxx:8000//bea.exe', 'C:\bea
.exe'); C:\bea.exe -m xxx.xxx.xxx.xxx -a
4PivFzWYe4frjqxzivXZ3eju9LBnmAURs8BckjkMZ4NbyjGYpy9T2fRm2LfQPwsy
```

Q: 安装了 agent 在云主机内，为什么在管理中心看不到新接入的工作负载?

A: 接入失败存在以下情况，

1. 当接入的工作负载总数超过了授权允许的接入总数或者授权已经到期，将无法接入新的工作负载，请联系厂商获取新的授权。确认是否因为授权限制，可以登录到页面后在右上角的“admin”查看“系统管理”。

2. 因为授权码无效或者客户端安装失败造成接入失败，可查看在客户端安装过程中的提示信息是

否失败，也可以查看/opt/dynarose/log/nodeclient.Info 文件是否有授权失败信息

Q: 如何确定是否在云主机内安装自适应微隔离的 agent 客户端成功?

A: Linux 环境下安装过程提示 nodeclient、collectclient 和 fwclient 服务正常即安装成功，如下图所示

```

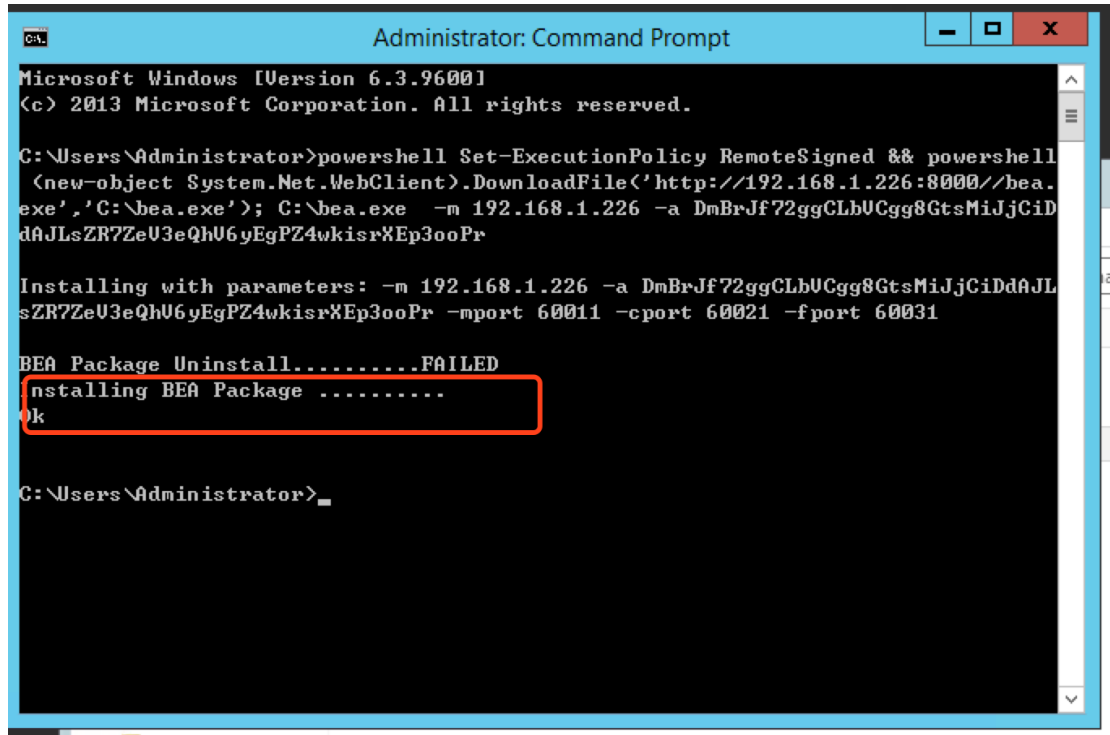
*****
*          安装 DYNAROSE 程序包开始          *
*****
检查操作系统和版本.....
当前系统是 Ubuntu [bionic]
检查是否存在旧的安装程序，并尝试移除.....
开始构建安装必备信息.....
开始构建安装源 Repo.....
创建 Repo 文件 /etc/apt/sources.list.d/dyn_repo.list
创建 Repo 文件完成
刷新安装源旧的 Cache 信息.....
开始安装程序包.....
开始安装程序包 nodeclient，请等待.....
程序包 nodeclient，安装完成.....
检测程序包 nodeclient，安装正确 OK.....
检测程序包 nodeclient，服务正常 OK.....
开始安装程序包 collectclient，请等待.....
程序包 collectclient，安装完成.....
检测程序包 collectclient，安装正确 OK.....
检测程序包 collectclient，服务正常 OK.....
开始安装程序包 fwclient，请等待.....
程序包 fwclient，安装完成.....
检测程序包 fwclient，安装正确 OK.....
检测程序包 fwclient，服务正常 OK.....
结束脚本执行.....END
    
```

如果是安装一段时间后查看是否 agent 客户端工作正常，请使用 `ps aux | grep client`，如下图所示三个 client 正常存在即为正常

```

ubuntu@ubuntu:~$ ps aux | grep client
root    10647  0.0  1.2 577268 12336 ?        Ssl  03:31   0:00 /opt/dynarose/bin/collectclient
root    10835  0.0  1.3 722748 13872 ?        Ssl  03:31   0:00 /opt/dynarose/bin/fwclient
root    10862  0.0  1.7 499156 18008 ?        Ssl  03:31   0:00 /opt/dynarose/bin/nodeclient
ubuntu  10968  0.0  0.1 13136 1116 pts/0    S+   03:36   0:00 grep --color=auto client
    
```

Windows 环境：在 administrator 权限下的 cmd 安装，安装过程提示安装 OK 为完成安装，如下图所示。



```
Administrator: Command Prompt
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

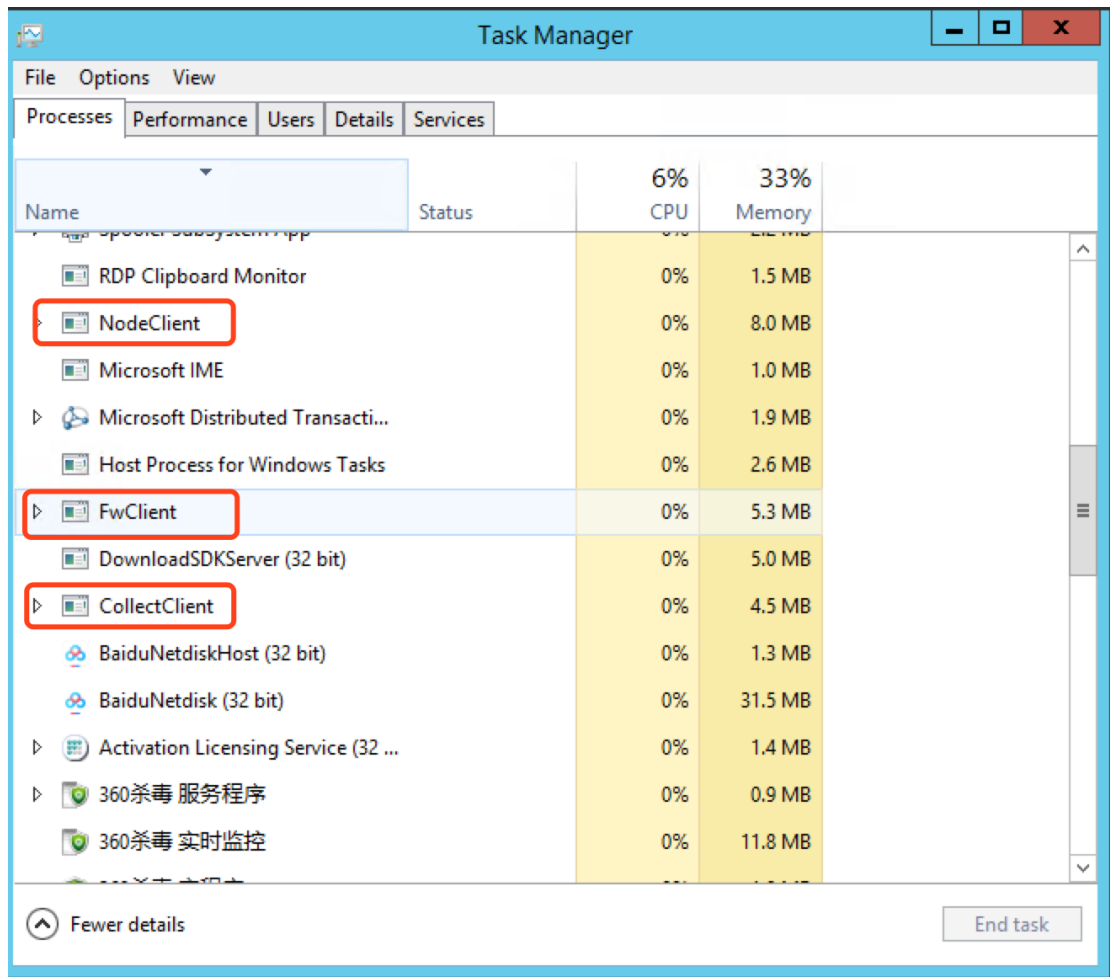
C:\Users\Administrator>powershell Set-ExecutionPolicy RemoteSigned && powershell
(new-object System.Net.WebClient).DownloadFile('http://192.168.1.226:8000//bea.
exe','C:\bea.exe'); C:\bea.exe -m 192.168.1.226 -a DmBrJf72ggCLbUCgg8GtsMiJjCiD
dAJLsZR7ZeU3eQhU6yEgPZ4wkisrXEp3ooPr

Installing with parameters: -m 192.168.1.226 -a DmBrJf72ggCLbUCgg8GtsMiJjCiDdAJL
sZR7ZeU3eQhU6yEgPZ4wkisrXEp3ooPr -mport 60011 -cport 60021 -fport 60031

BEA Package Uninstall.....FAILED
Installing BEA Package .....
Ok

C:\Users\Administrator>
```

或者在任务管理器中看到 nodeclient、collectclient 和 fwclient 三个任务也可判定安装成功。如下图



Q: 为什么配置了策略工作负载没有启动防护的作用?

A: 可能存在两种配置缺少情况造成, 1) 检查是否将配置的新策略发布, 通过查看页面右上角倒数第二个图标 (为发布图标), 如果有显示数字代表还有配置未被发布, 不会被生效到工作负载上, 所以请点击发布图标或者进入到菜单点击“安全策略管理”=>“更新发布”, 提交发布说明就可以发布了。2) 可能没有将相应的工作负载切换到“防护”模式, 在业务拓扑和工作负载列表两个页面都可以查看对应的工作负载是否开启了“防护”模式, 只有防护模式才能够启用此工作负载的防护作用。

Q: 业务拓扑图的红色线和绿色线都代表什么?

A: 业务拓扑图上的红色线代表工作负载被访问的流量连接与微隔离的策略没有匹配, 当工作负载切换到防护, 红色的流量连接将会被阻断; 业务拓扑图上的绿色线代表工作负载访问的流量连接与微隔离的策略可以匹配上, 当工作负载切换到防护, 绿色的流量连接将会被放开允许访问。

Q: 自适应微隔离的 agent 支持的操作系统有没有详细的版本列表信息?

A: 主要支持两种类型系统 Windows 和 Linux,

Linux 支持环境: Centos6、7 Ubuntu12、14、16 (LTS only) RedHat6、7 Debian7、8、
9SUSE 11、12openSUSE 12、13、42

Windows 支持环境: Windows Server 2008 R2、2012、2012 R2、2016。(注: 以上各版本 64
位系统) Windows7、10

Q: 如何获取并导入新的 License, 并使 License 生效?

A: 首先需要 ssh 登录到安装自适应微隔离的云主机系统内, 进入到/opt/dynarose/License 目录
内, 执行 genreqkey 会生成 license.req 文件, 请将文件或者文件的内容发送给我们的客服人
员, 客服人员会根据此文件生成授权文件 license.lic 文件, 当得到此授权文件请将 license.lic
文件放置到/opt/dynarose/sysadmin/cfg/目录下, 并执行此命令 docker restart
dynarose_sysadmin_1, 执行成功后可在 web 控制台页面查看“系统管理”的信息来校验是否
License 生效成功。