天翼云·微隔离防火墙

用户使用指南

天翼云科技有限公司

1 产品介绍

1.1 产品定义

微隔离防火墙（CT-MIFW Micro-isolation Firewall）面向云化数据中心的跨平台统一安全管理软件，能够对数据中心的内部流量进行全面精细的可视化分析和高细粒度的安全策略管理；能够帮助用户快速便捷的实现环境隔离、域间隔离以及端到端隔离，与云下一代防火墙互补，实现纵深防御

1.2 产品优势

1）基础架构无关

与基础架构无关，与系统适配

- Linux 发行版
  - CentOS: 5.X(有限支持)/ 6.X/ 7.X/ 8.3.2011
  - Ubuntu: 14/ 16/ 18.04 LTS/ 20
  - Debian: 8/ 9/ 10
  - Suse: 11.4/ 12-SP1/ 12-SP5
  - Open Suse: 42.3/ 13.2/ Leap-15.0
- Windows Server
  - Windows Server 2008R2
  - Windows Server 2016
  - Windows Server 2019
- 国产操作系统
  - UOS:V20-Debian10/V20-CentOS7.7/V20-CentOS8.2
  - Kylin: V4/ V7/ V10
  - EulerOS: SP5
  - OpenEulerOS: 20.09/ 21.09
- 容器平台
  - K8S+Docker
  - K8S+CIR-O

2）系统影响小

- 采用安全可靠架构设计
  a) 全用户态设计，不侵蚀系统内核
  b) 单向控制通信，不额外开放端口

c) 客户端防卸载、防删除、防停用

- 智能优化系统性能开销
  a) 连接、阻断关系合并上报
  b)防火墙策略对象智能聚合
- 多项资源占用保护机制
  a)CPU 单核占用率降级阈值设定
  b)连接、阻断关系内存占用限制
  c)Conntrack 最大容量动态调整
  d)TCP / UDP 超时时间智能调整

3）管理规模大

多规格集群模式满足高性能及可用性需求

集群规格	集群模式	最大纳管规模
双机集群	双主	2000 虚机/3000 容器
4 机集群	2 接入+2 数据	10000 虚机/15000 容器
6 机集群	2 接入+4 数据	20000 虚机/25000 容器
8 机集群	2 接入+2 管理+4 数据	30000 虚机/40000 容器

产品价值或亮点

自适应安全的核心理念在于持续的监控（continuous monitoring）和分析，并根据分析结果持续的调整具体的策略配置。而监控的目标，可以是各个层面的各种信息，包括网络，应用，内容，终端设备，人员属性等等。

1、减少数据中心内部被攻击风险

2、提升业务交付时间

3、安全策略集中可视化管理

4、简化网络流量

5、减少运维成本

6、混合云统一安全管理

7、漏洞攻击面风险量化分析与屏蔽

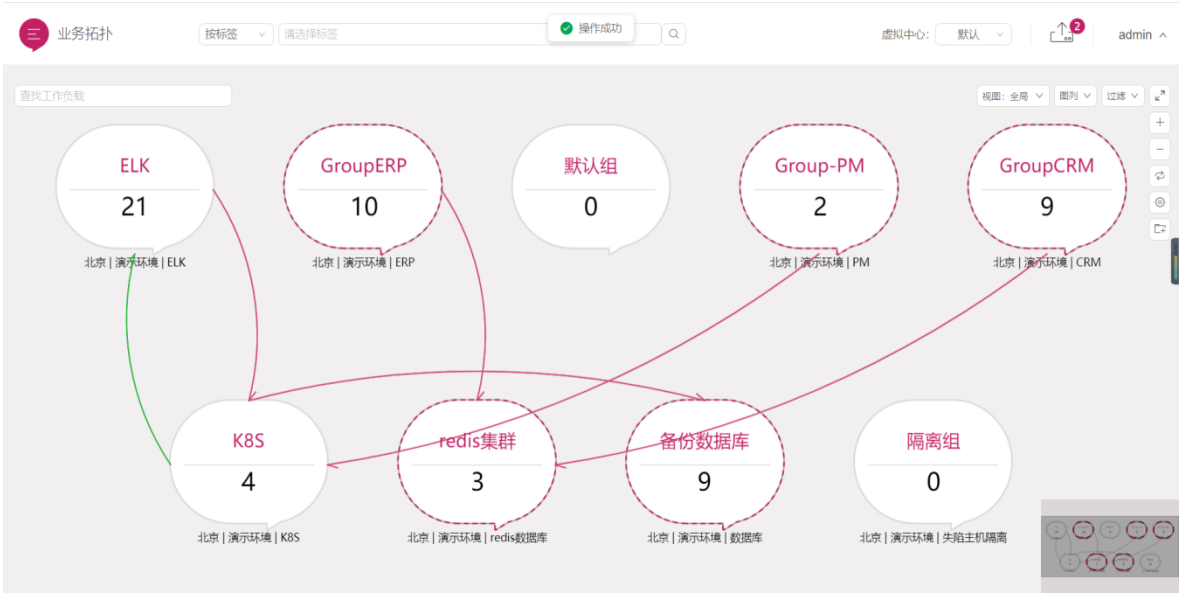
8、协助满足等保 2.0 要求

1.3 功能特性

1） 工作负载标签化管理

零信任访控需要面向身份，微隔离的控制需要面向业务，这二者的关联是什么？对于“非人实体”而言，他的身份其实是他的业务角色，这一点其实与“真人实体”并没有什么差异（小张、小李不是身份，这个人的业务角色才是授予他权限的依据）

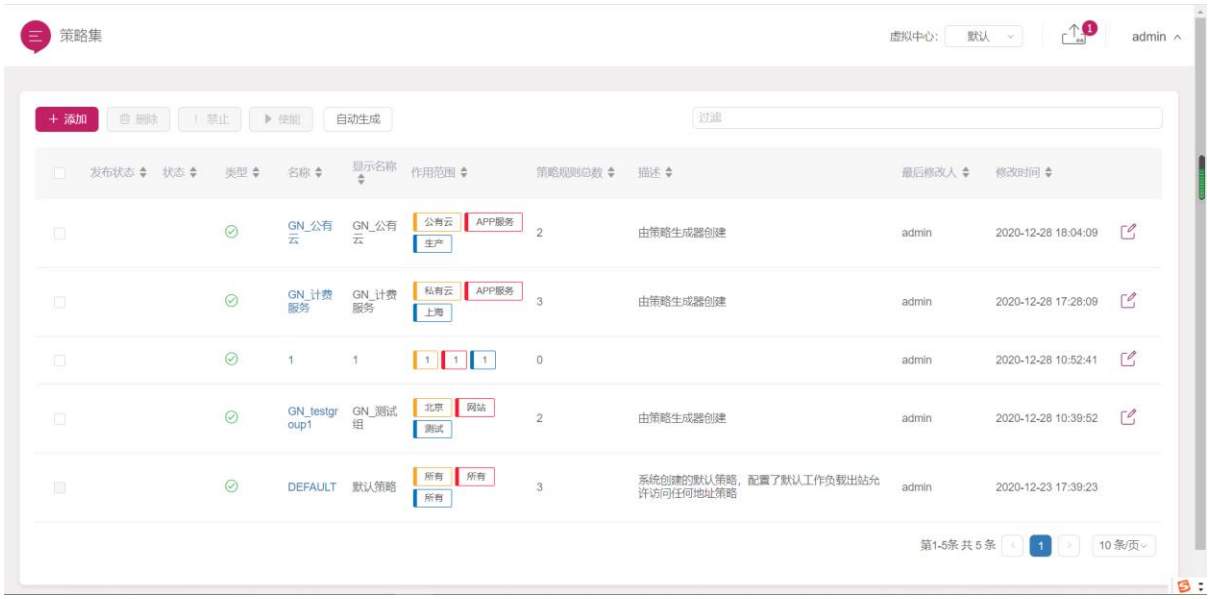
- 工作负载标签化管理，是指基于多维属性标签，刻画工作负载业务角色、标定工作负载资产身份的管理设计。标签化是实现基于业务的互访流量可视化、面向业务的访问控制和自适应策略计算的基础能力；
- 通常情况下，可通过工作负载的位置、环境、应用、角色等属性定义标签；
- 在进行策略配置时，我们是通过标签的组合来设定策略控制的范围的。所以，从工作负载本身、到带有多维标签的身份、再到使用多维标签的策略范围，我们通过四层实体、三次动态映射实现了安全策略与基础设施解耦（即面向业务而非基础设施）。



2) **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%。

当我们理清了内部连接的基线模型后，就要开始进行策略配置了。东西向流量的策略配置复杂度比较高，我们也进行了针对性的设计：

- 首先，上面提到策略是基于标签而配置的，一方面实现了安全策略面向业务（而非基础设施），另一方面则大幅减少了基于 IP 地址的策略规模，降低了系统运算量及性能开销；
- 其次，我们的策略具有多种模式，具备建设、测试、防护 3 种策略生效模式，最大化的降低安全策略部署过程中的业务影响；
- 第三，我们可以通过多种方式配置策略，比如在可视化试图中点击连接线，向导式的快速放通某个连接，又比如我们可以提供一个策略生成器，将当前的策略效果与实际发生的连接进行匹配，帮助客户分析出目前的策略配置没有覆盖到的连接，进而快速、批量的生成策略；最大化降低使用难度。
- 第四，对于有特殊需求的终端，我们也支持基于 IPSec 协议实现点到点的加密，最大化实现灵活管控。

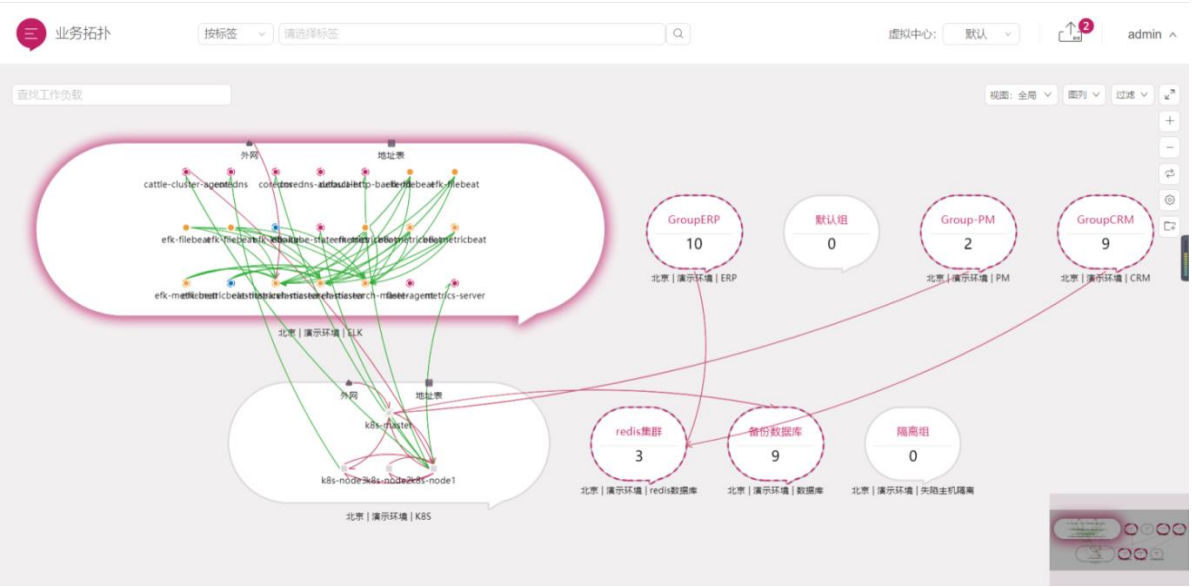


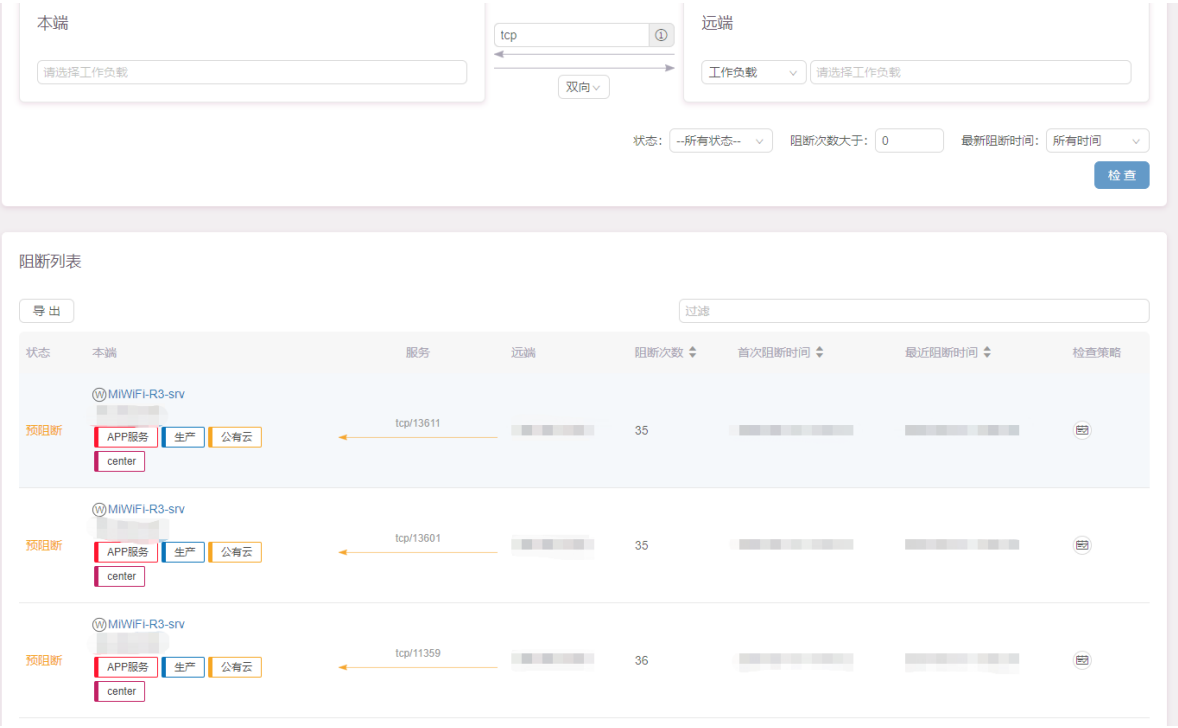
3) **安全策略可视化管理：**在业务拓扑中利用红绿线标识符合策略的流量及不符合策略的流量，并支持查看流量阻断日志。

由于我的工作负载都带有业务角色的属性，所以就非常有利于我基于学习到的连接关系，生成一张综合的可视化试图，可以直管呈现环境间、业务间、工作组间、工作负载间的互访关系。

基于这个能力，给我们带来了多方面的价值：

- 有利于我们梳理资产、摸清家底，知道我有哪些工作负载，知道工作负载开放了什么端口（暴露面），护网时我们就经常利用这个功能生成资产台账和端口台账；
- 便于以学习到的情况为基础，清晰的梳理内部的互访关系。
- 业务连接可视化分析解决了管理者对数据中心东西向流量不可视、无感知的难题，同时也是进一步确定流量基线，部署访问控制策略的依据。





4) **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。

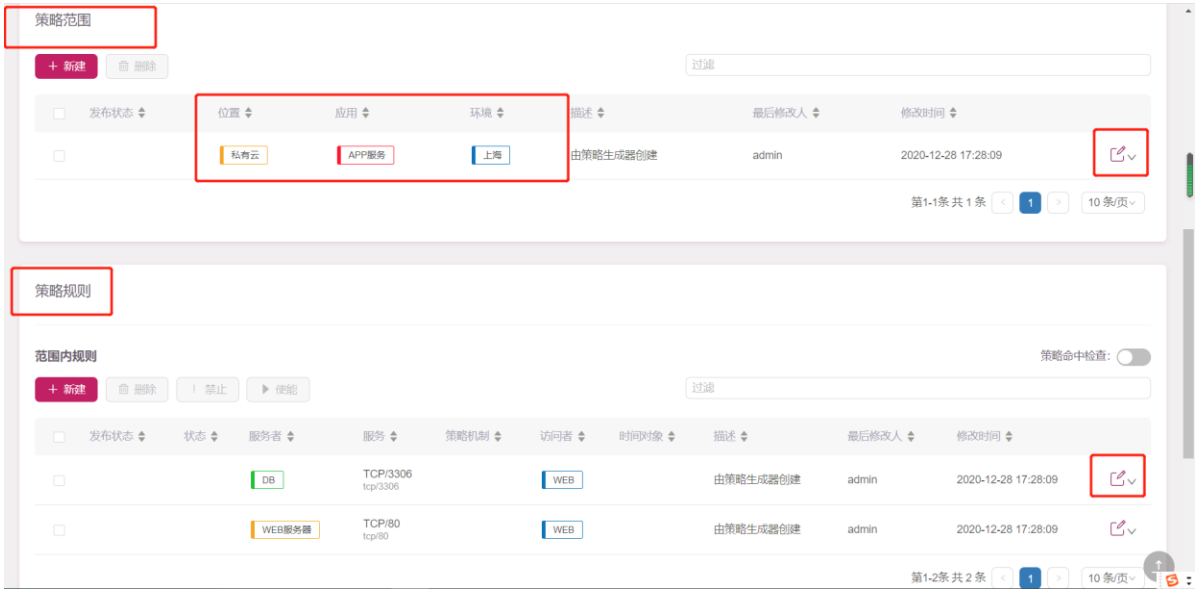
全局策略自适应计算，是指微隔离系统根据工作负载的变化而自动调整符合其业务角色的安全策略。这样的场景在云化数据中心中时常发生，如业务从物理机迁移至虚拟机、新的数据中心建设、新的业务上线、动态扩缩容等。

这里我们示例了一种最简单的策略自适应计算场景：

1.用户基于标签，使用接近自然语言的描述配置一条策略；

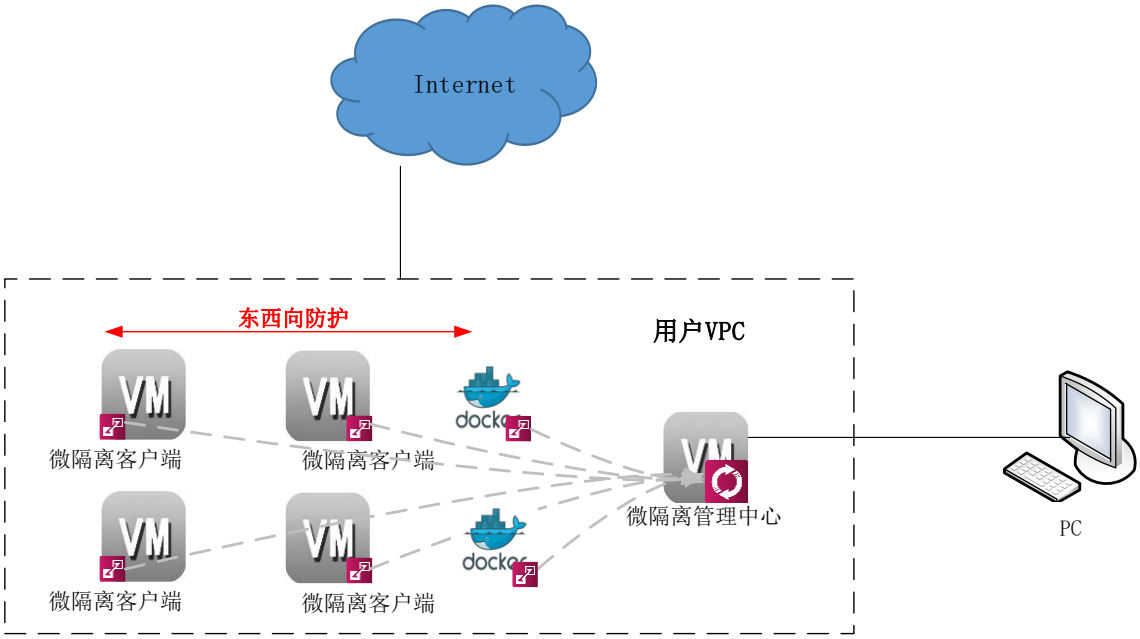
2.自适应策略计算引擎将标签翻译为对应的 IP 地址；

3.当某一个工作负载发生 IP 变化时，BEA 迅速上报该信息，自适应策略引擎则基于这个变化快速进行策略计算，并将新的策略下发至相关工作负载上。



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。

1.4 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。

a) 网站病毒与异常行为发现

适用于金融、运营商、互联网、政企、能源电力、Jundui 网络病毒与异常行为发现及防护，能够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。

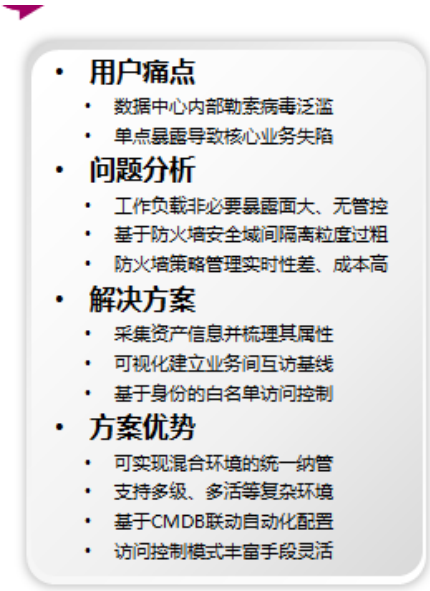
b) 业务可视化及端口管理

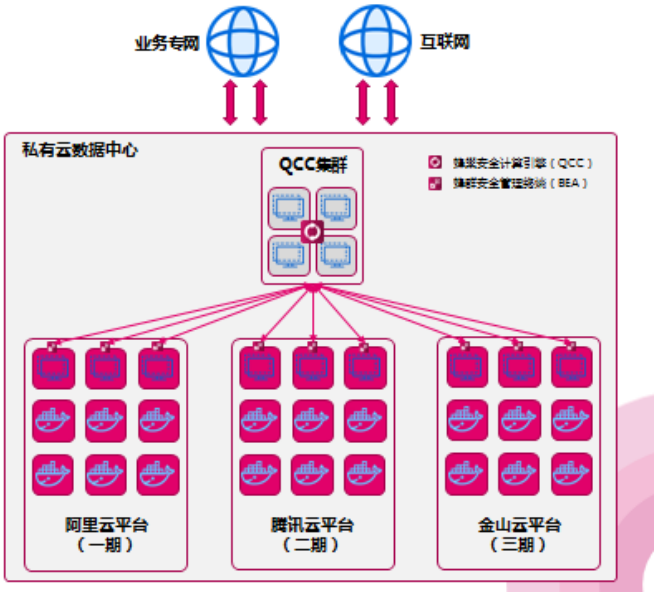
适用于金融、运营商、互联网、政企、能源电力、Jundui 业务可视化及访问控制端口管理，业务主机开放了多种业务端口服务，需要可视化业务流量与服务端口，实现访问关系授权与端口台账。

c) 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。

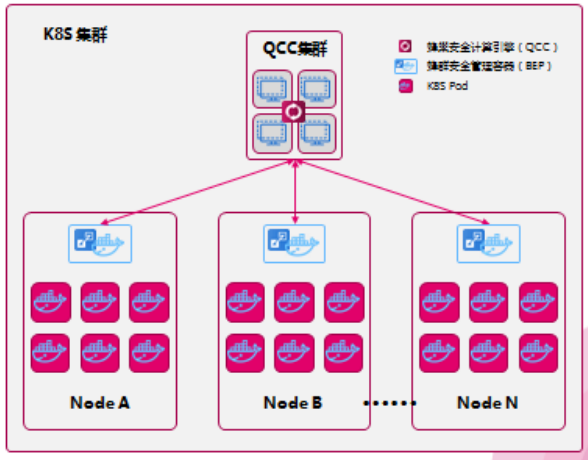
1） **数据中心内部隔离及访问控制解决方案应用**





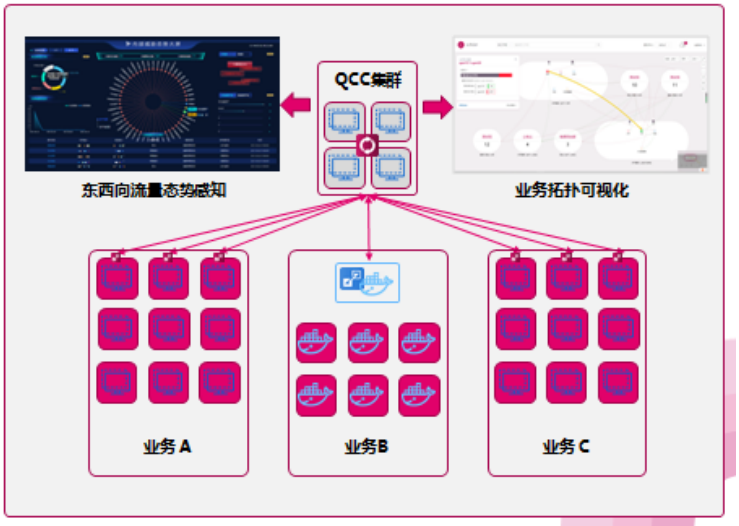
2) **容器网络隔离与控制解决方案应用**

- **用户痛点**
  - 容器互访关系错综复杂无法梳理
  - 内部暴露面大、核心业务风险高
- **问题分析**
  - 云原生环境连接复杂且漂移频繁
  - 传统防火墙无法适应云原生架构
  - Network Policy管理操作不友好
- **解决方案**
  - Daemonset方式部署控制端
  - 基于API自动化标定容器角色
  - “5步法”实现最小业务授权
- **方案优势**
  - 适应云原生环境、提供容器化部署
  - 自动化标签设置、自适应策略计算
  - 基于自学习及可视化辅助策略设计
  - 实现跨域异构混合环境的统一纳管

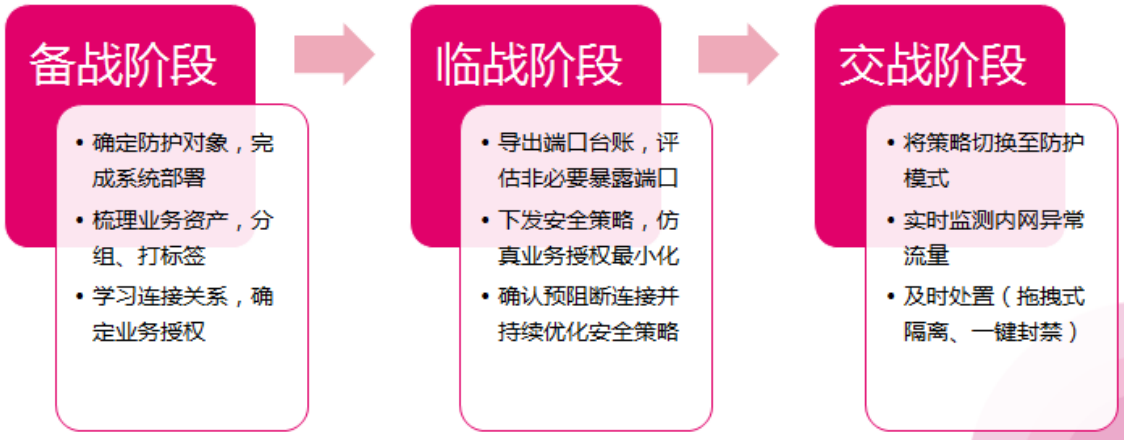


3) **数据中心东西向流量监测与分析解决方案应用**

- **用户痛点**
  - 梳理不清内部互访，业务运维困难
  - 无法洞察内部异常，检测分析低效
- **问题分析**
  - 缺乏感知内部流量的技术手段
  - 传统采集方案成本高、开销大
  - 难以建立连接与业务对应关系
- **解决方案**
  - 按业务对工作负载分组并标定角色
  - 以业务为单位可视化呈现连接、阻断、预阻断关系
  - 基于告警规则、异常模型监测异常
  - 通过API向态感平台同步连接数据
- **方案优势**
  - 部署效率高，资源占用小
  - 可建立资产、业务、连接对应关系



4) **护网及重保内网加固解决方案应用**



5) **等级保护 2.0 基本要求应对方案**

安全通用要求

8.1.3 安全区域边界

8.1.3.2访问控制

a) 应在网络边界或区域之间根据访问控制策略设置访问控制规则，默认情况下除允许通信外受控接口拒绝所有通信；（网络白名单）
b) 应删除多余或无效的访问控制规则，优化访问控制列表，并保证访问控制规则数量最小化；（业务与策略一致）
c) 应对源地址、目的地址、源端口、目的端口和协议等进行检查，以允许/拒绝数据包进出；（点到点访问控制）

8.1.3.3 入侵防范

a) 应在关键网络节点处检测、防止或限制从外部发起的网络攻击行为；
b) 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（防范内部威胁）

8.1.4 安全计算环境

8.1.4.4入侵防范

b) 应关闭不需要的系统服务、默认共享和高危端口；（主机网络应用白名单）
c) 应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制；（堡垒机防绕过）

云计算环境扩展要求

8.2.3.2 入侵防范

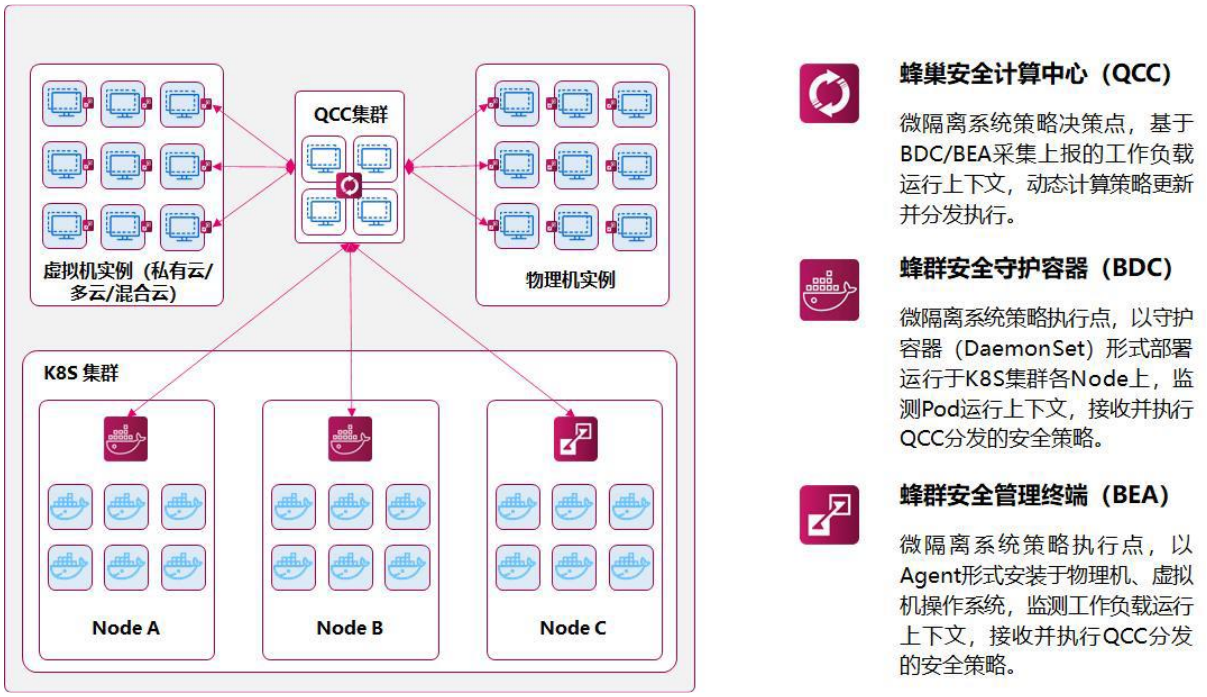
c) 应能检测到虚拟机与宿主机、虚拟机与虚拟机之间的异常流量；（虚机间流量识别）

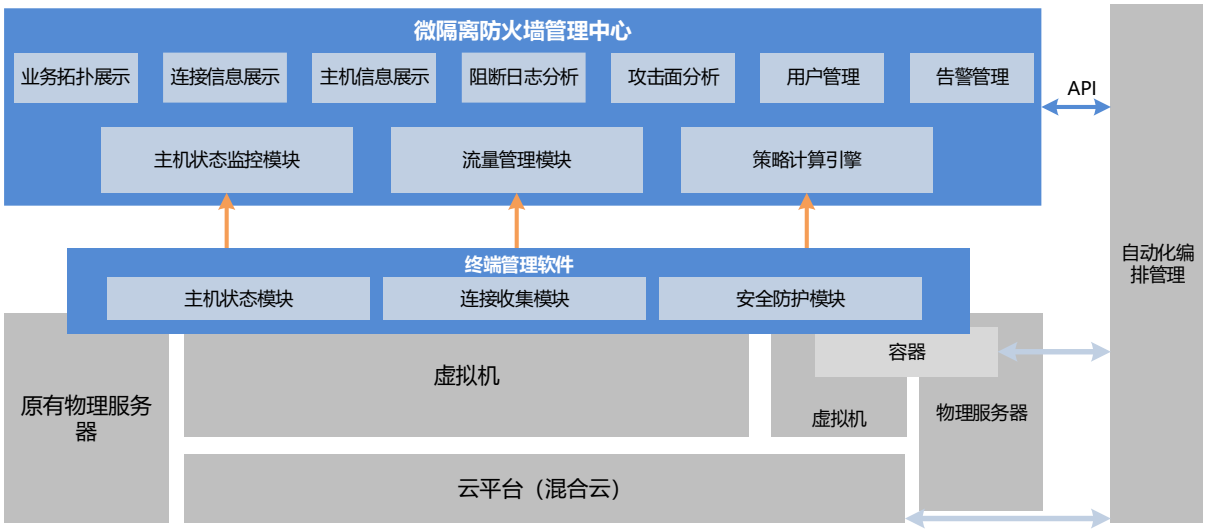
8.2.4.2 访问控制

c) 应保证当虚拟机迁移时，访问控制策略随其迁移；（策略自适应运维）
d) 应允许云服务客户设置不同虚拟机之间的访问控制策略；（点到点访问控制）

1.5 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。

授权码：指安装客户端时所验证匹配的校验码。

工作负载：泛指承载业务的主机，包含物理机、虚拟机、容器等一系列计算主机的统称。

工作组：通过“位置“，”应用“，”环境“三维标签来确定一个工作负载的集合。

连接线：工作负载之间互相访问的路径，通过计算引擎计算后显示在 web 界面的线。

策略：针对工作负载之间，工作组之间的访问流量设置白名单的方法。

策略状态：指创建策略应用至工作负载或工作组的状态，分别为建设状态，测试状态，防护状态。

建设状态：只在管理中心生效的策略状态，用于策略制定，该状态下策略不会应用至工作负载。

测试状态：策略下发至工作负载，但不生效，会记录所创建的策略，不对业务产生影响，该状态下适用于测试策略是否正常的情况。

防护状态：在工作负载上应用，且只允许创建的策略通过，未指定策略的访问流量将无法通过。

角色标签：对工作负载的业务或其他条件定义的标签，弱化 IP 的依赖，从业务的角度赋予工作负载的名称，方便后期策略的制定和使用。

组标签：组标签用于定义一个工作组，分别是位置，应用，环境。

访问者：指访问的发起方，即访问来源。

提供者/服务者：指提供服务的工作负载，与访问者一同理解。

预阻断日志：在切换成测试状态时，工作负载记录到的不符合策略（未阻断）的流量日志。（工作

负载需开启日志收集）

阻断日志：在切换成防护状态时，工作负载记录到的不符合策略（被阻断）的流量日志。（工作负载需开启日志收集）

2 计费说明

2.1 计费模式

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 价格与订购

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%

订购

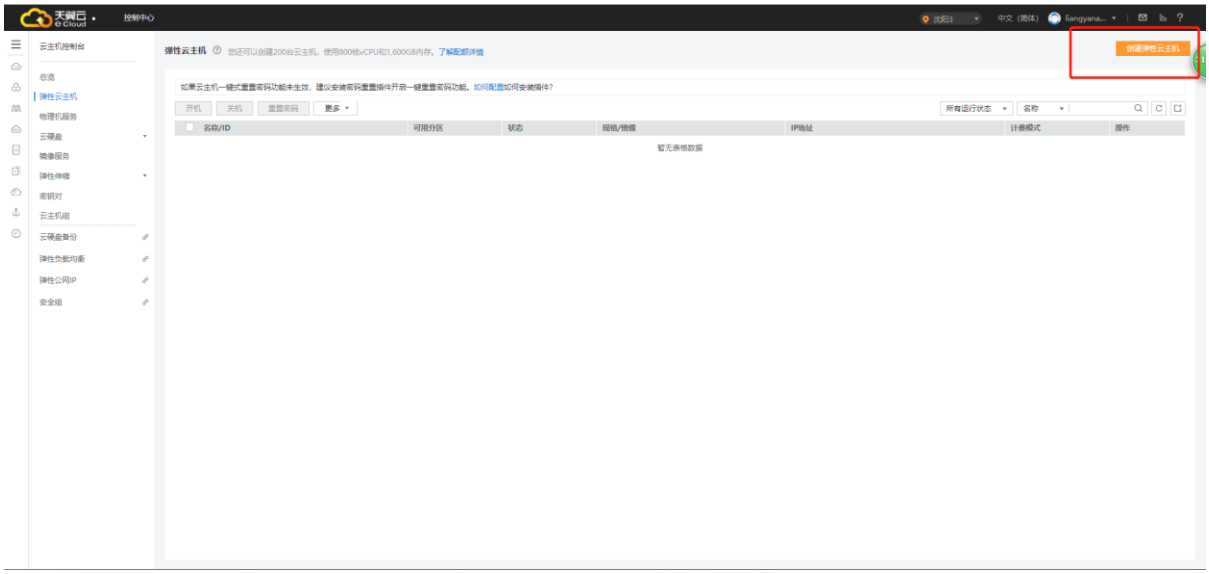
微隔离防火墙以镜像方式承载，订购前需要开通一台云主机承载业务，然后再购买授权。

操作步骤如下：

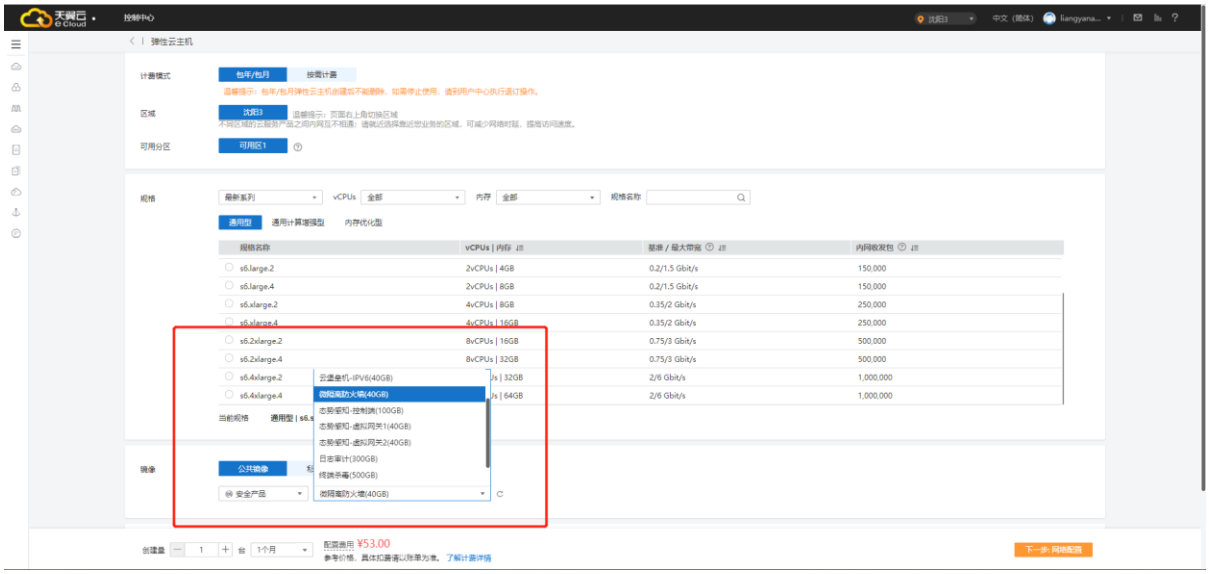
1、进入天翼云官网，点击右上角【控制中心】。

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。

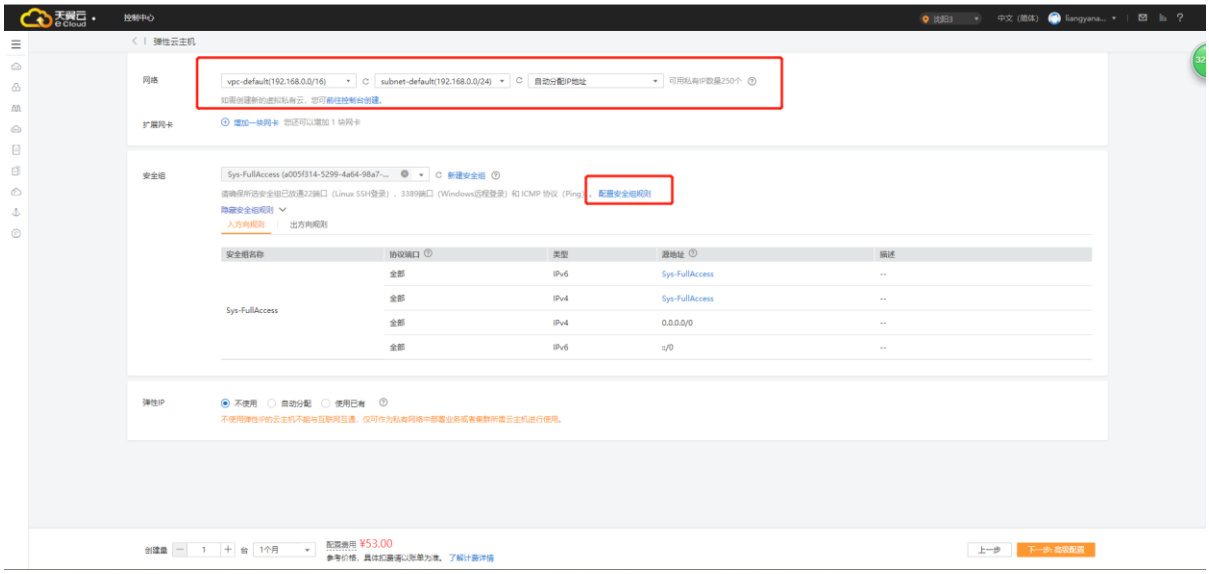


5、云主机需开放端口：10443、6443、8000、60001、60011、60021、60031 端口。6443 为 WEB 控制台访问端口，10443 端口为后台管理使用的端口，8000 安装 agent 的访问端口，60001、600011、60021、60031 为 agent 接入自适应微隔离管理中心的使用端口。

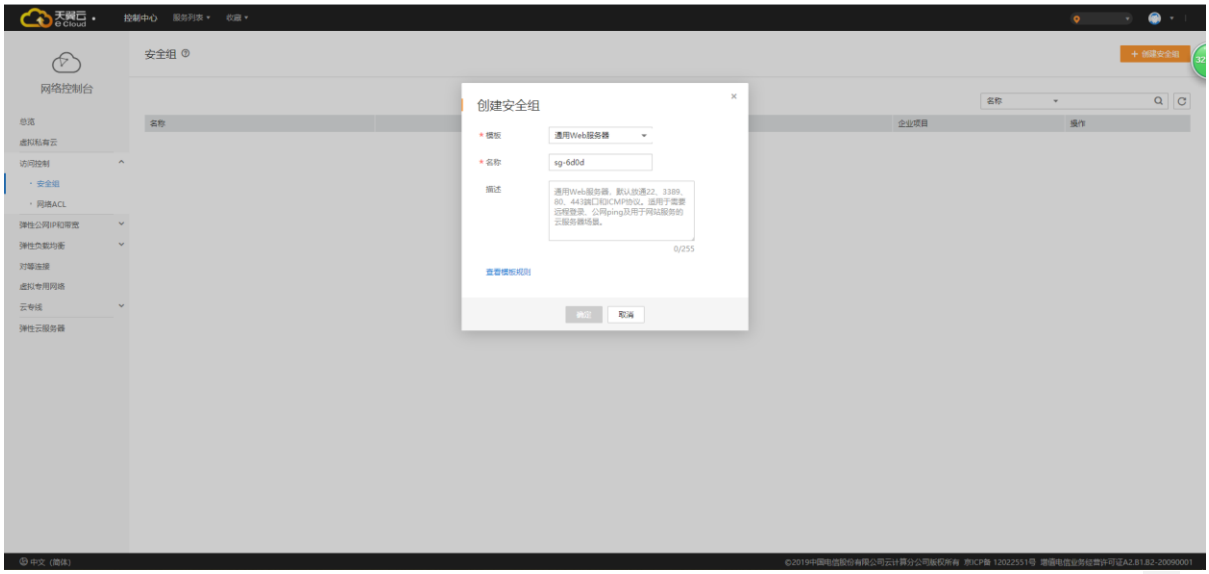
开放端口操作：

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 4.2.1 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。

2.3 升级与续订

升级操作是在 cosole 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

续订

续订操作是在 cosole 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。

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 快速入门

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）

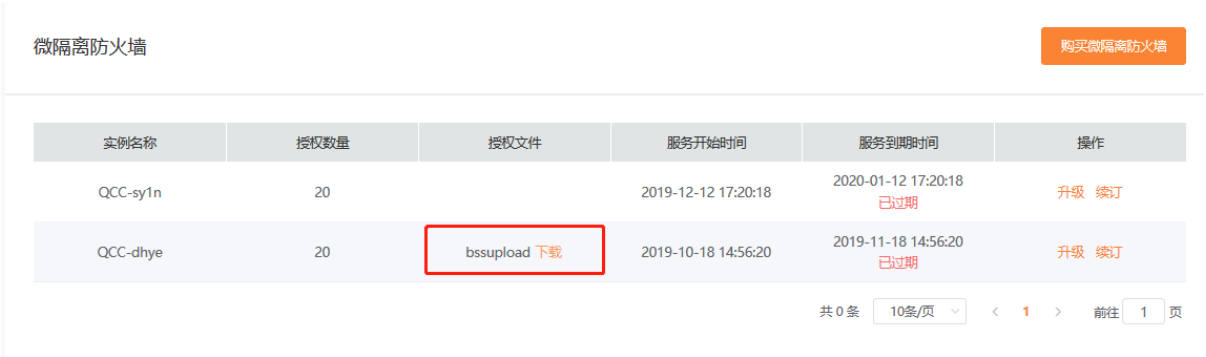
产品采用 web 页面进行管理及操作，在浏览器输入“https://+管理地址：映射的端口”即可进入登录界面，

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

默认用户名和密码：**请联系 400 客服咨询。**

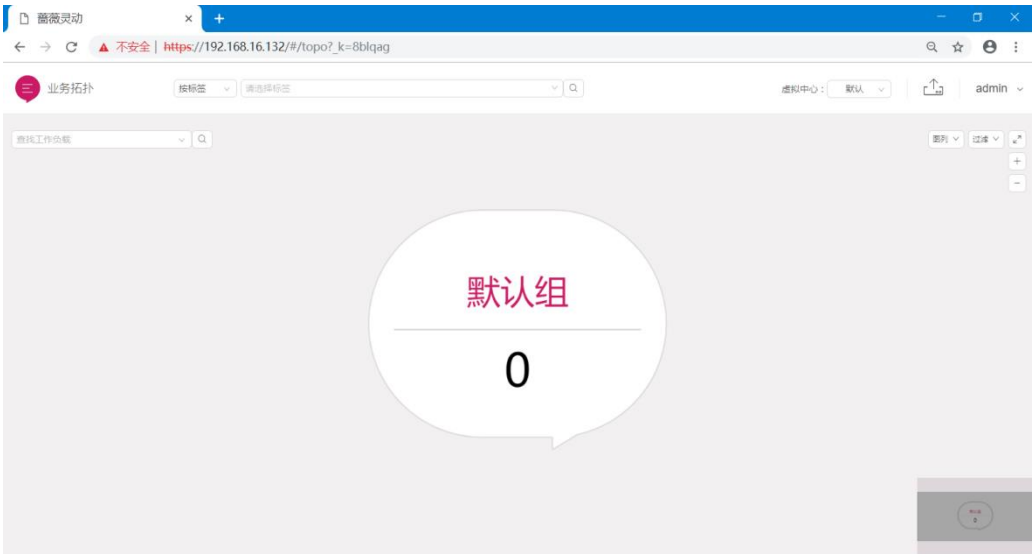
默认密码在受理完成后，产品控制台实例列表中下载，如下图所示。



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。管理员账号被锁定后只能联系厂家解锁，其他用户被锁定，可登录管理员账号，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

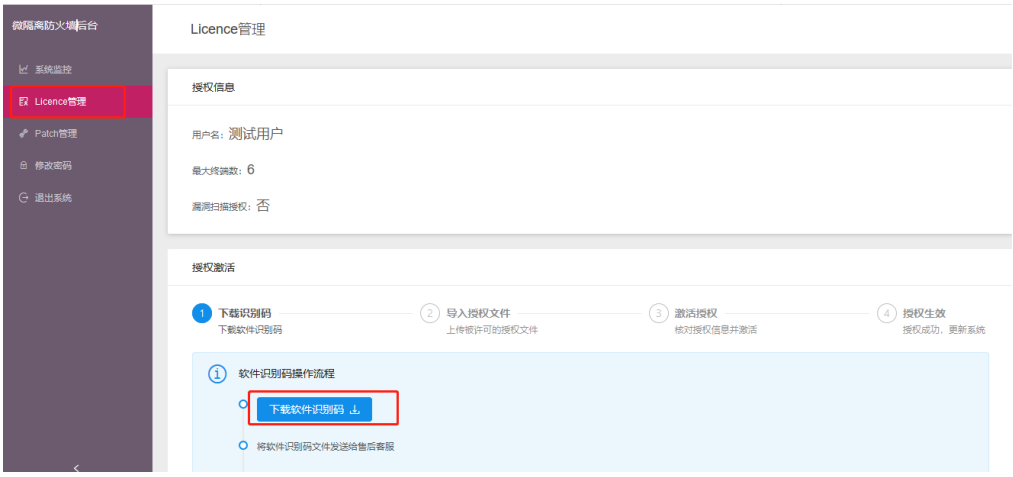


3.2管理中心（QCC）授权

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。

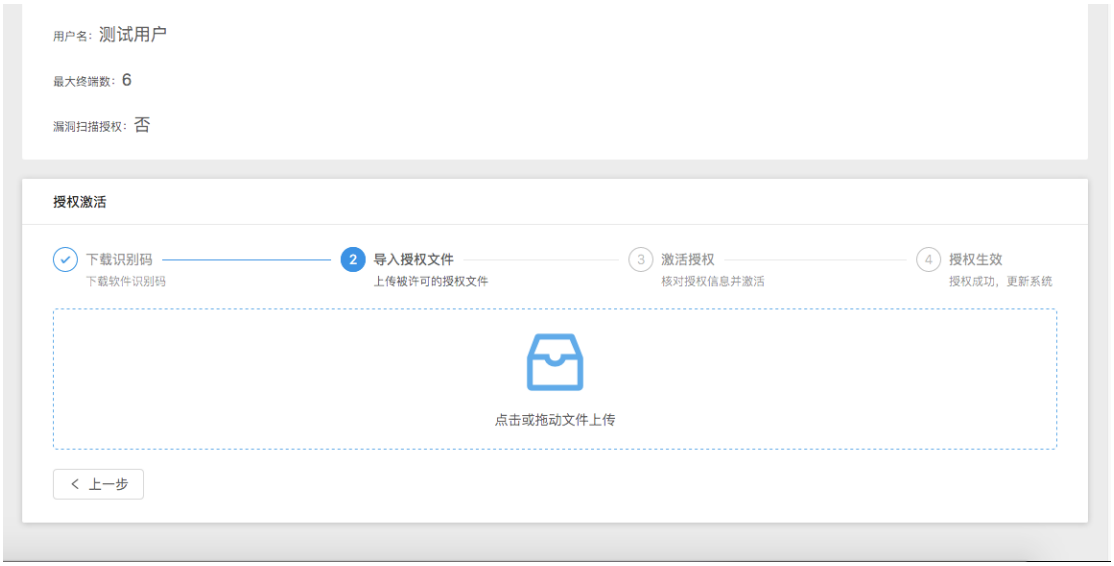


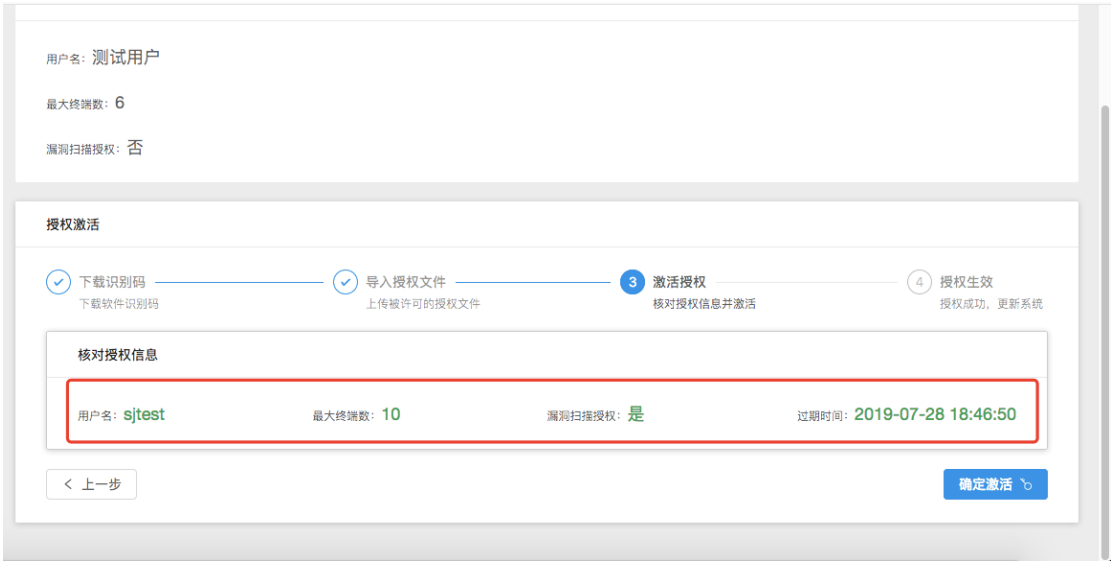
3.2.2 获取授权文件

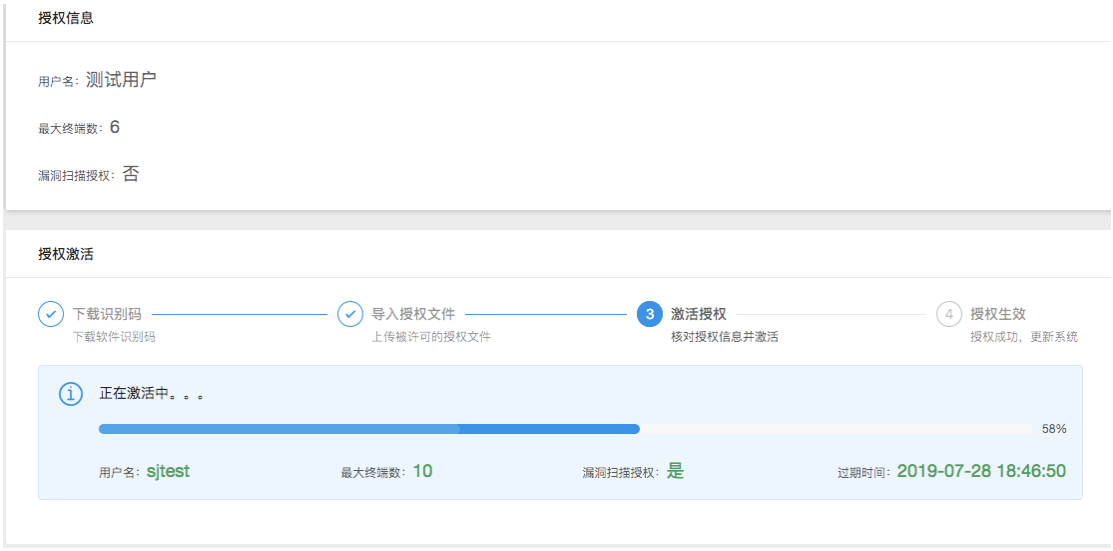
将所下载的软件识别码发送给售后服务人员，售后服务人员将根据服务订单信息制作授权文件。制作好的授权文件将可通过邮箱、邮寄或其他方式传递给用户。

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。





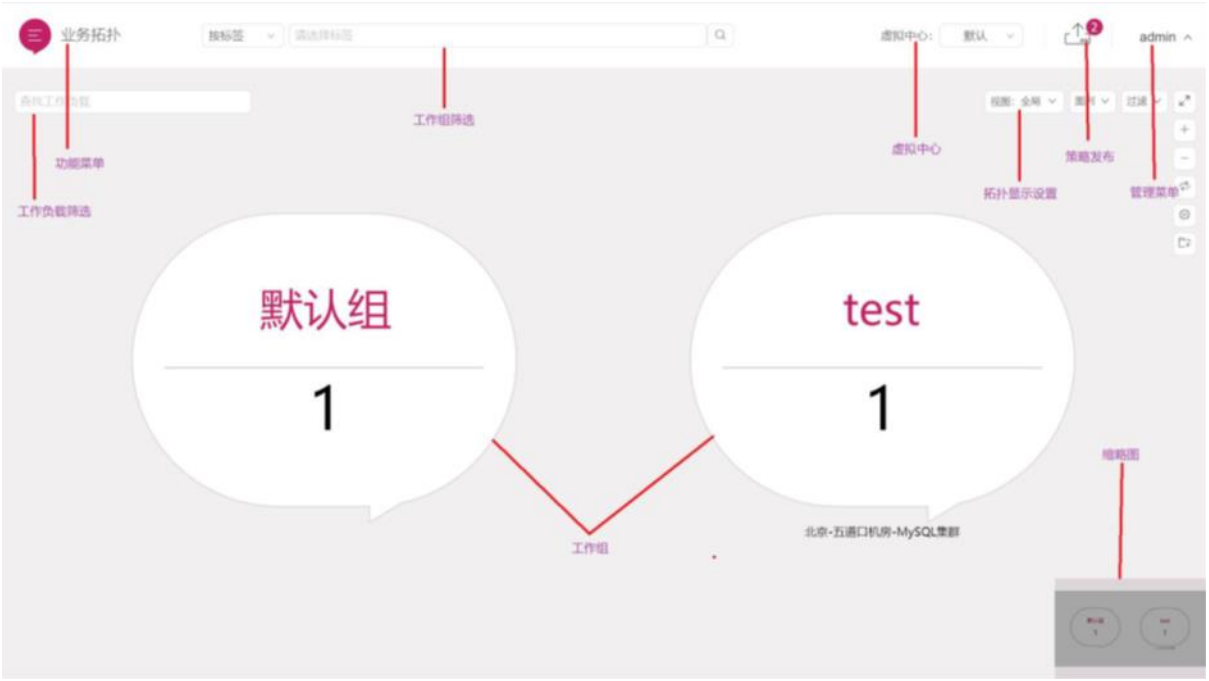


授权成功后可在 licence 管理中查看系统授权信息。

3.3 日常操作管理

系统默认的日常操作登录地址为 https://+管理 IP：6443

首次登录后进入的主界面是业务拓扑图，图中《默认组》即是一个工作组，默认组在新安装产品时默认存在，安装 BEA 后，工作负载会在页面显示，工作组是 1-3 个标签定义的工作负载的集合，类似于传统安全中的安全域，业务组等概念。下图为首界面的相关说明，界面的具体讲解会在 4.1.2 业务拓扑进行说明。



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. 1. 1. 1　新建组标签

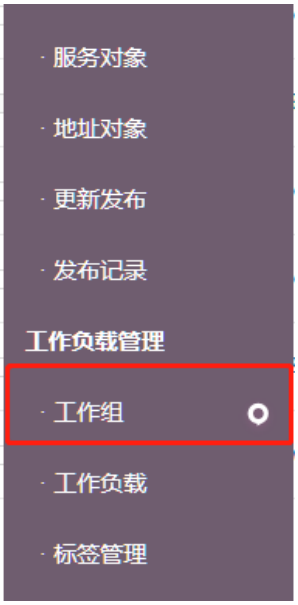
1.首先点击菜单栏的标签管理：

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）。

4.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。

3.1.1.2 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。

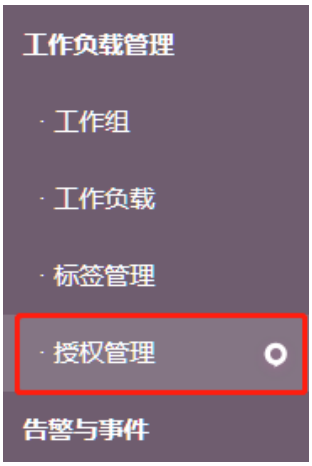
注：当工作组无标签时，无法匹配策略。

4.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）

3.1.1.3 创建授权码

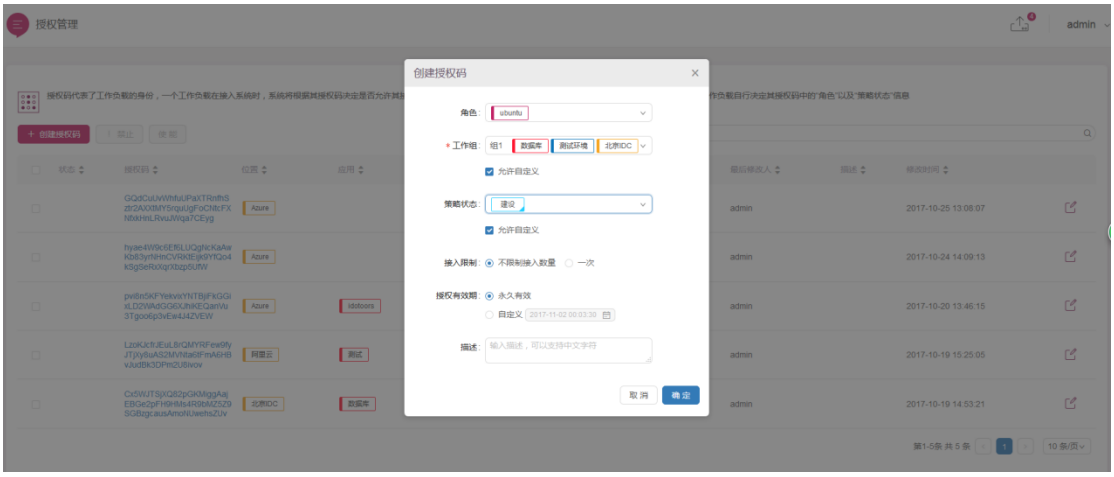
1.创建授权码有两个入口，一个是菜单栏的授权管理，通过此入口可以查看管理所有授权码。



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）。

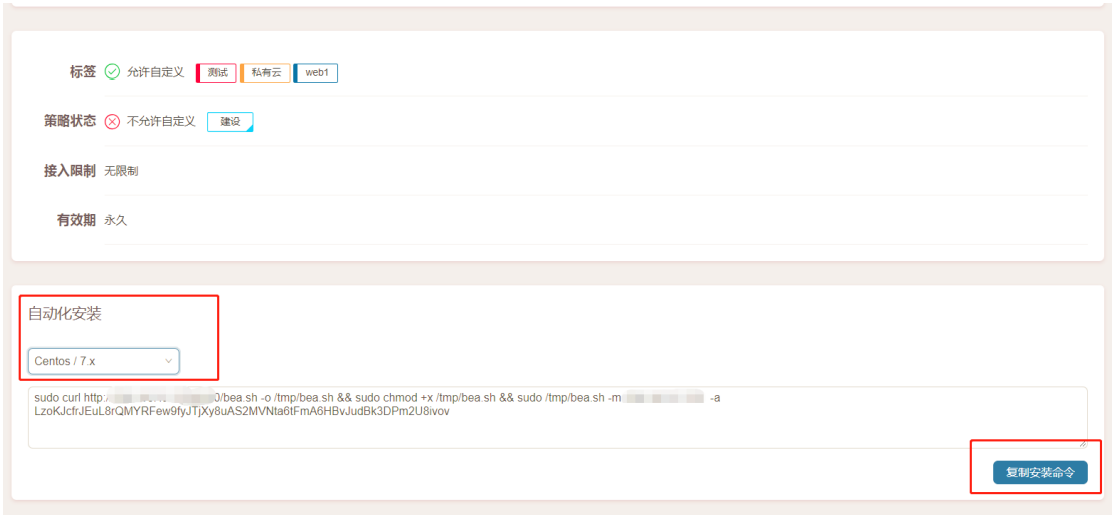
2.创建授权码

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。



3.点击授权码，可进入授权码详细页面。

4.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。



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。

4.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。

3.1.1.4 接入工作负载

-Linux 系统,在自动化安装处选择对应的 Linux 系统版本复制生成的安装命令,生成安装命令后，点击复制按钮，粘贴至具备 root 用户权限的命令行终端中，即可进行安装。

-Windows Serve，在自动化安装处选择对应的 windows 系统版本，生成安装命令后，点击复制按钮，粘贴至具备管理员权限的 cmd 中，即可进行安装。。

-也可以使用自动化运维工具进行批量安装。

登录页面查看 agent 是否接入成功，功能菜单→ 工作负载管理→工作负载，即可查看接入的工作负载。

注意：

1. 执行安装命令，系统会自动到管理中心获取安装脚本，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。若只在建设或测试模式下运行，可在安装命令后加-nf true ，则不安装 Agent 的微墙客户端（fwclient 防护模块）。

5.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。

6.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。

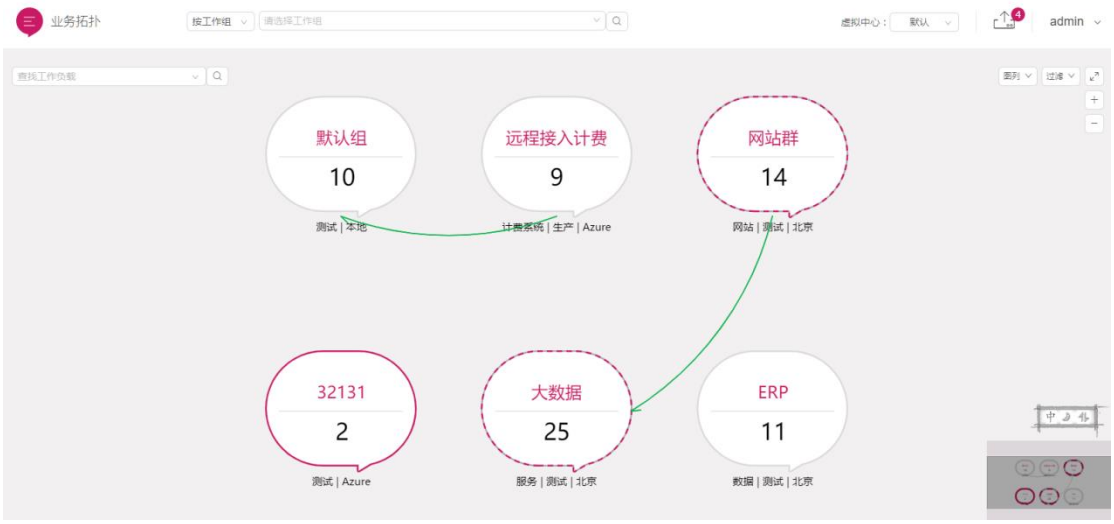
根据以上内容可以快速进入管理中并将需要管控的工作负载接入到管理中心（QCC）,工作组和配置防护策略以及各个模块详细功能需要参看**用户指南**。

4 用户指南

4.1 可视化分析使用说明

4.1.1 基本功能说明

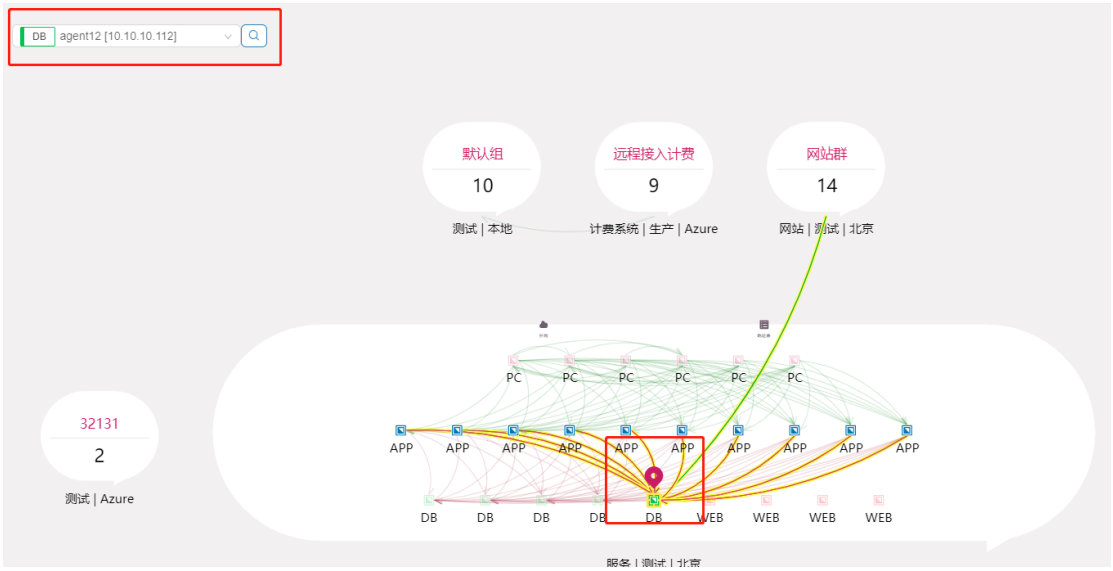
1.为了更好的展示及说明业务拓扑的功能及操作，以下使用已包含多台工作负载的微隔离防火墙进行说明。Demo 界面如下：



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。

4.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（位置，应用，环境）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。

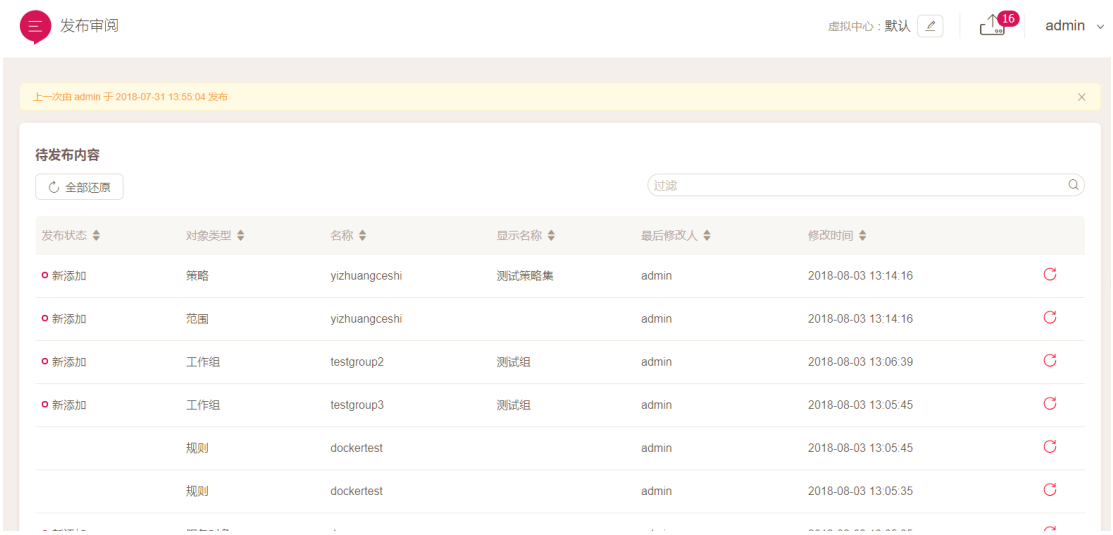


5.点击页面右侧的 

，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。



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。

未被策略允许：未配置合规的安全策略

被策略允许：已配置合规的安全策略

8.图例标识右侧的过滤 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， 标识可以使首页拓扑页面的工作组恢复初始排布序列， 标识可以对视图参数进行设置。

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。

4.1.2 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。

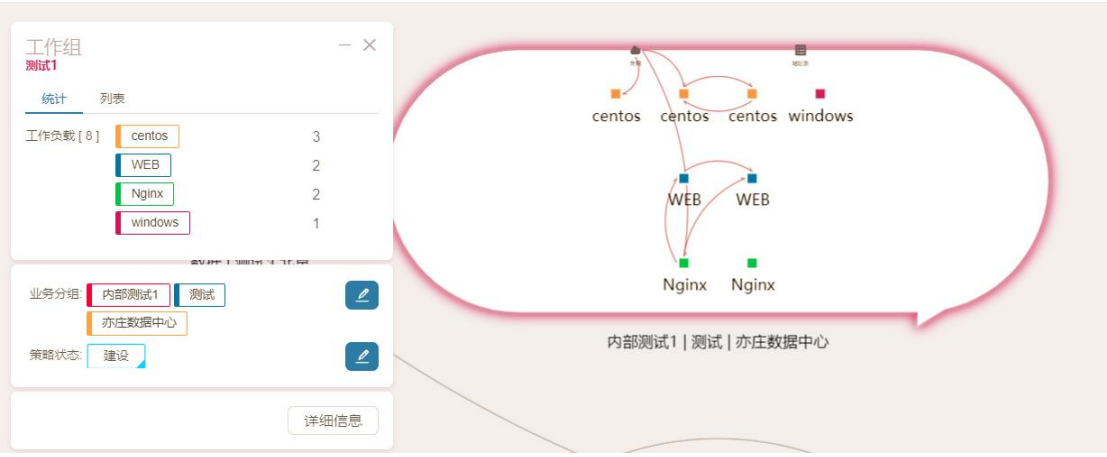
-单击工作组，可查看该组的基本信息。基本信息页面可以修改该工作组的标签及策略状态。

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。

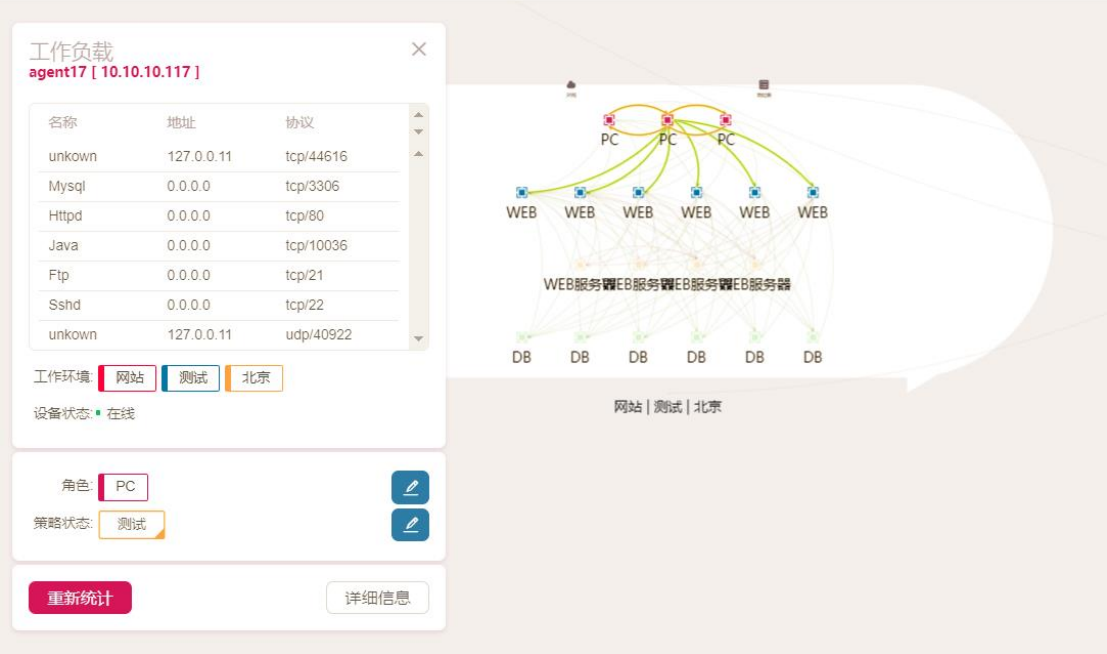
-双击工作组，可展开此工作组，并查看其中工作负载。



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。

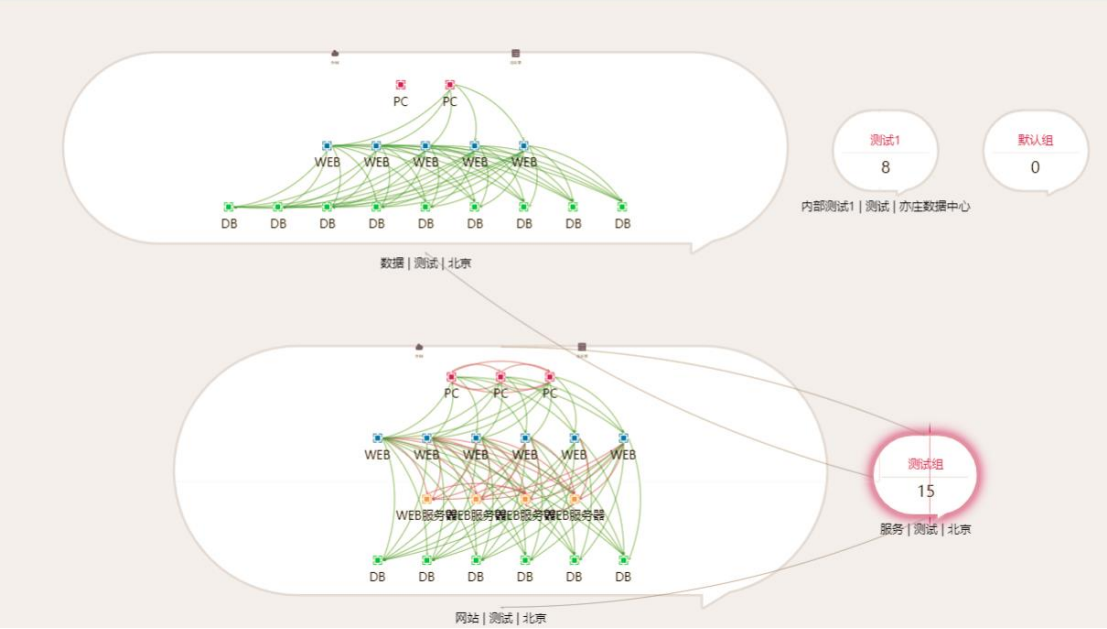


-在工作负载基本信息框中可快速修改该工作负载角色及策略状态。重新统计按钮可清空所有针对此工作负载的访问连接记录。

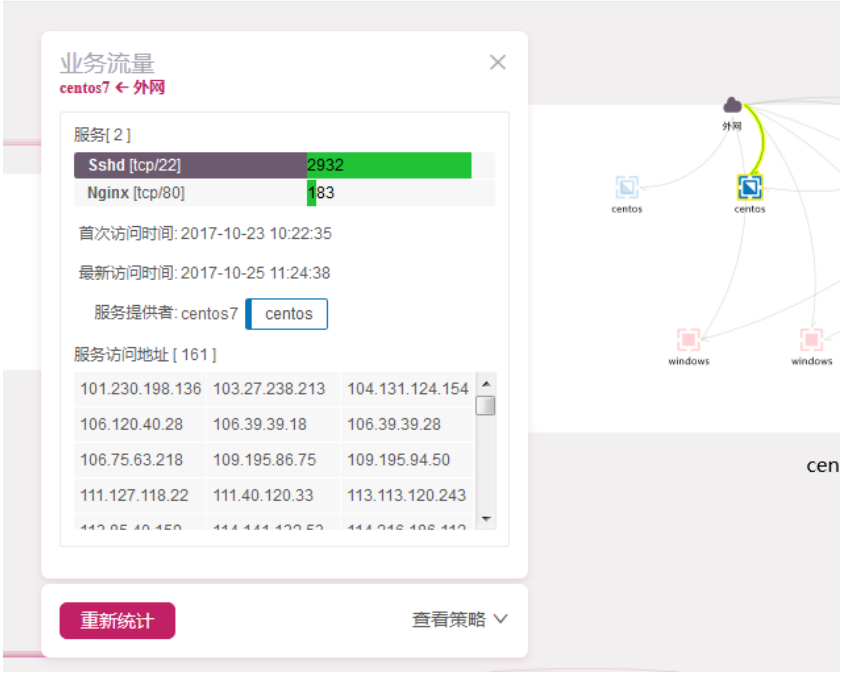
-支持在基本信息框中直接新建角色。

4.连接线

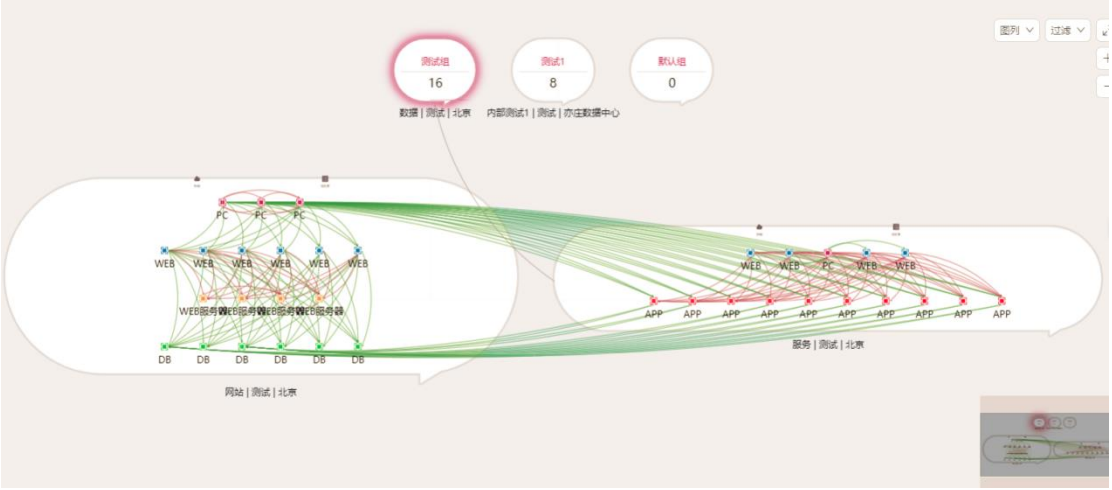
-拓扑中每条连接线均代表此元素对于工作负载的访问连接，拓扑中的元素包括外网、地址表、工作负载。



-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。



-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。



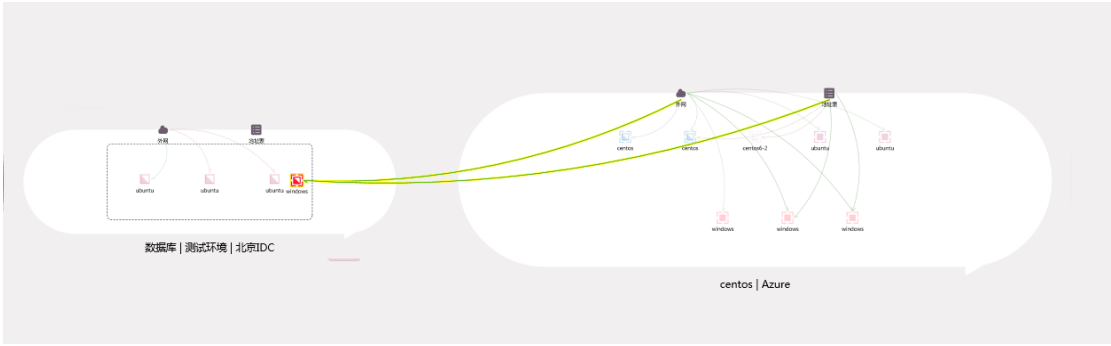
-红色连线说明此条连线中存在不合规的访问，绿色线为两元素之间的访问均符合规则。

-单击某条连线，还可直接查看或添加安全策略。

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。

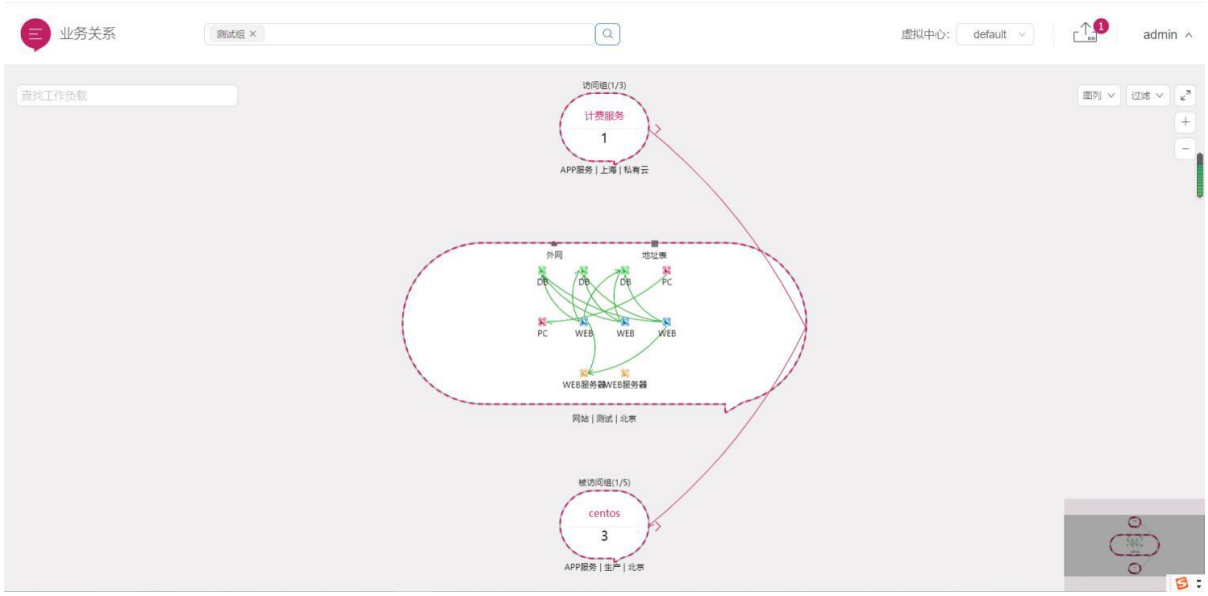


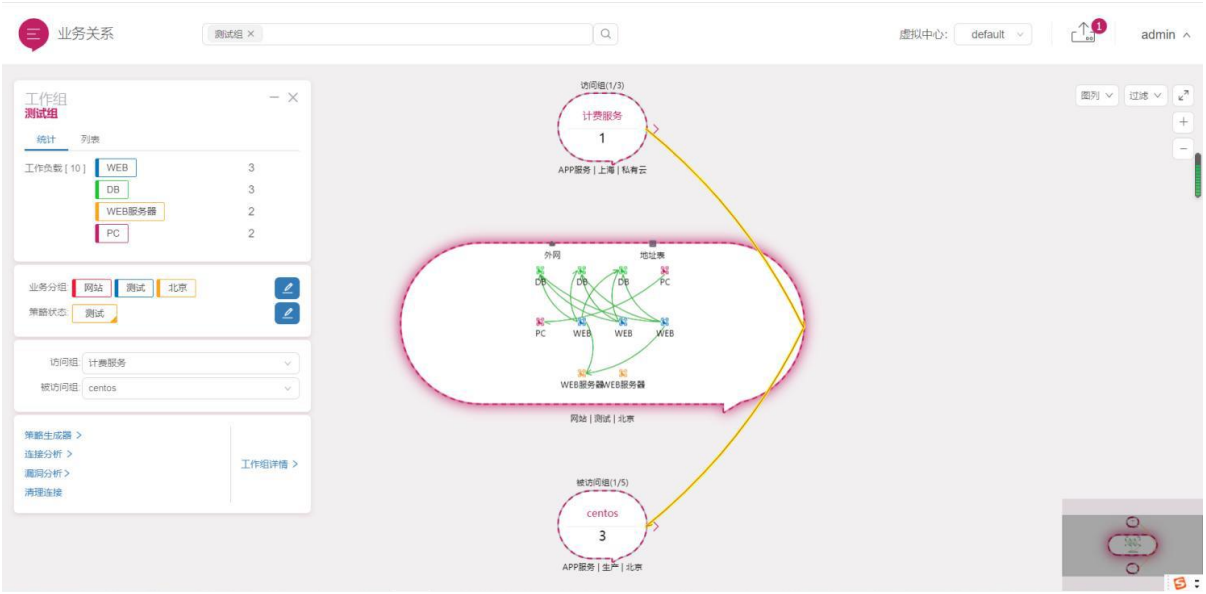
4.1.3 业务关系使用说明

点击功能菜单->可视化分析->业务关系，进入此功能界面。

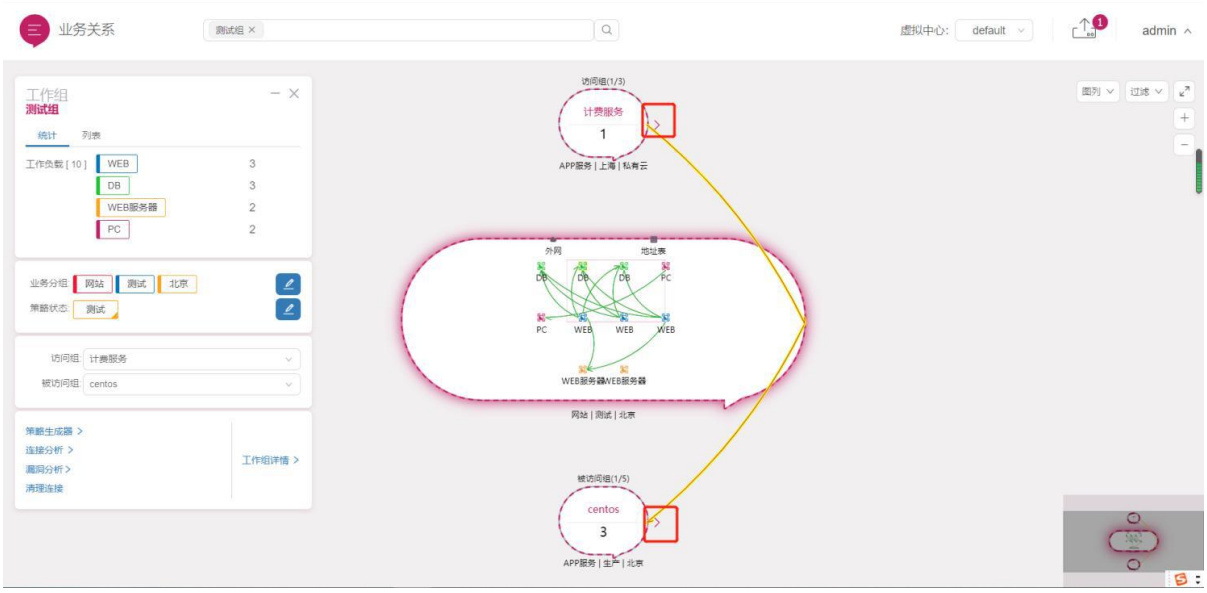
业务关系界面主要帮助用户对每个工作组的业务关系进行针对性的分析和梳理。

1.按照页面中的提示，选择一个工作组，可以看出该工作组中的工作负载的访问情况和被访问情况。

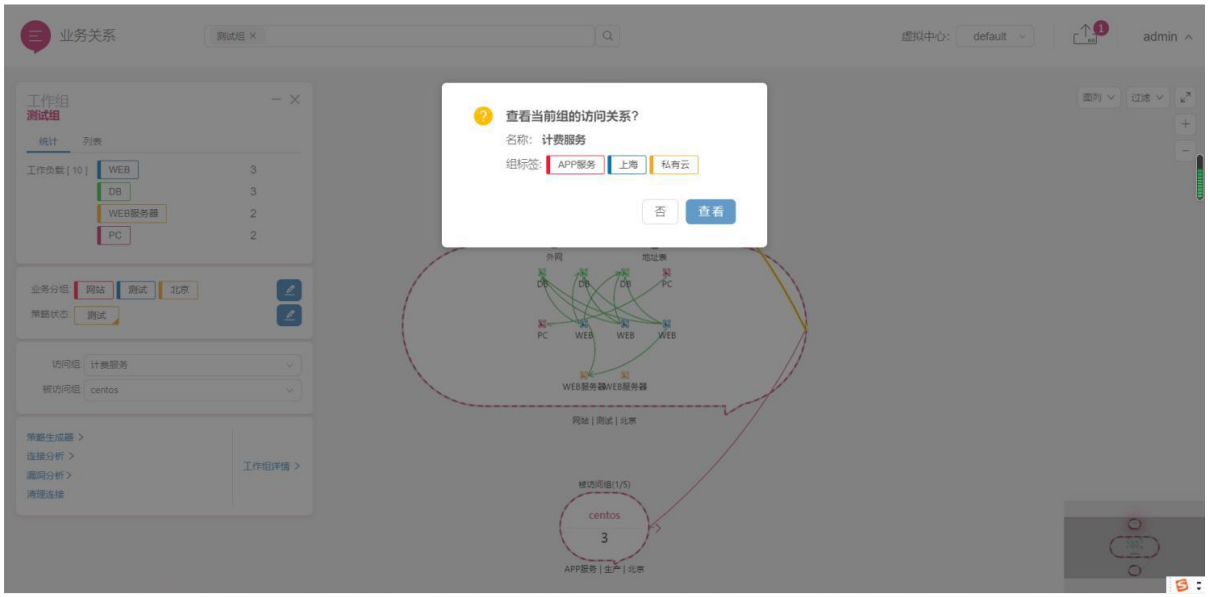




2.在访问组和被访问组有多个时，可以单击中间的工作组，点击红框中的下拉键，选择其他工作组。 或 者通过点击或选择查看工作组与该组间访问关系。



3.单击访问组或者被访问组，可以切换组视角，来查看该组的访问和被访问关系。

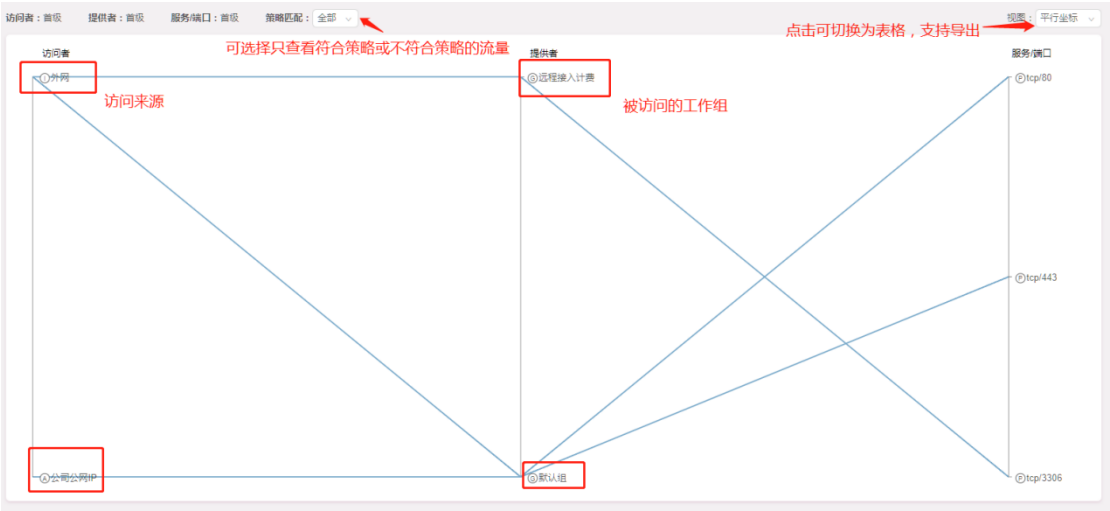


4.1.4 连接分析使用说明

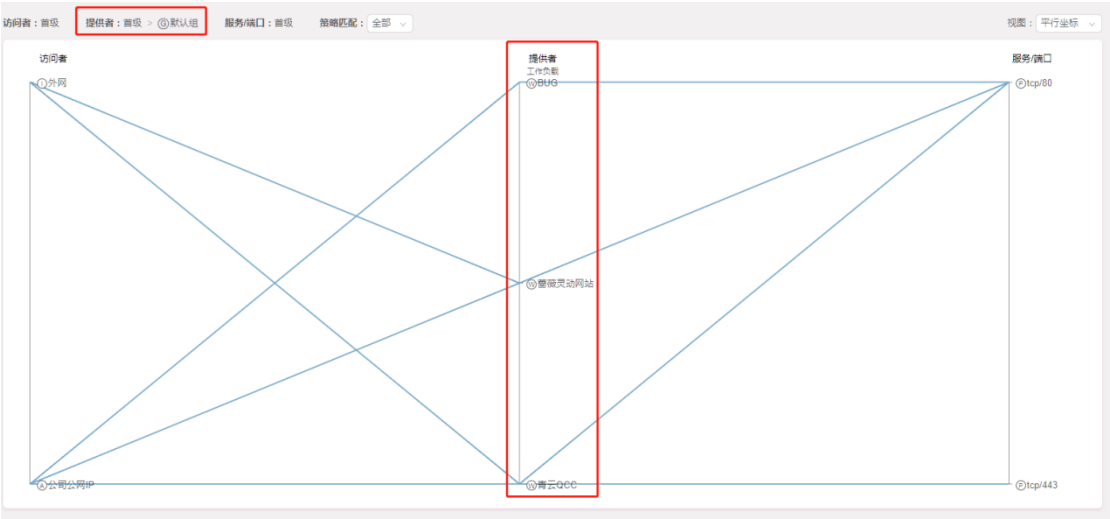
1.点击菜单栏-连接分析，可进入连接分析界面。连接分析页面可帮助用户对于内部流量有针对性的进行筛选、钻取、分析。

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。

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

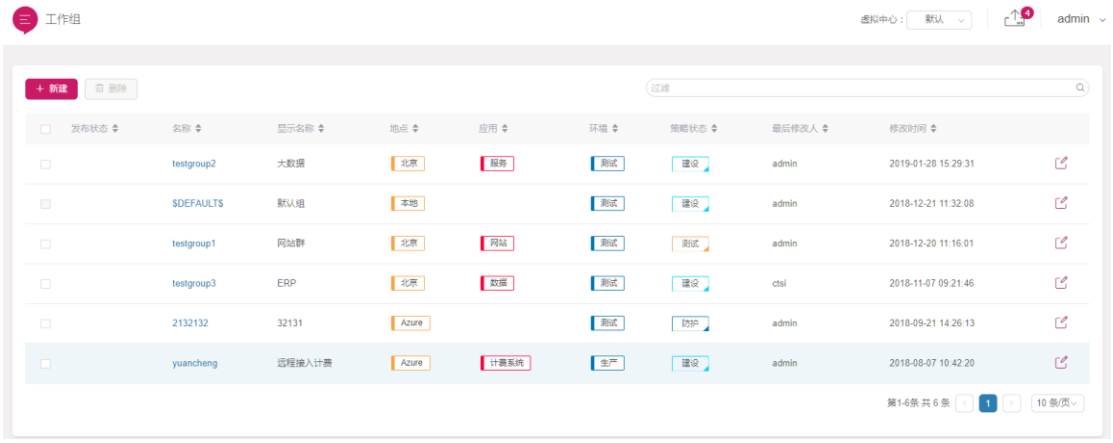


4.2 工作负载管理模块

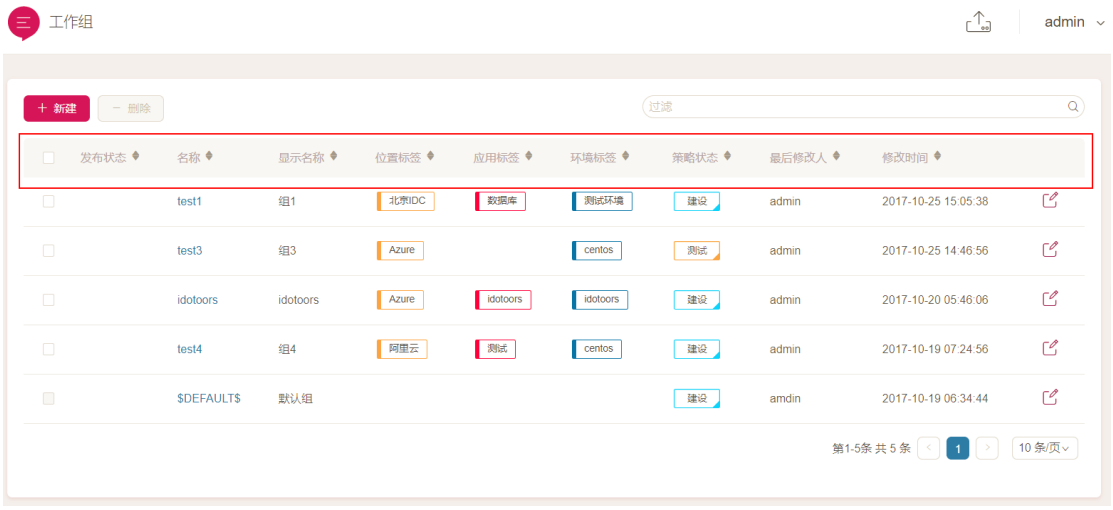
工作负载管理模块包含三个部分：工作组、工作负载、标签管理、授权管理

4.2.1 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。



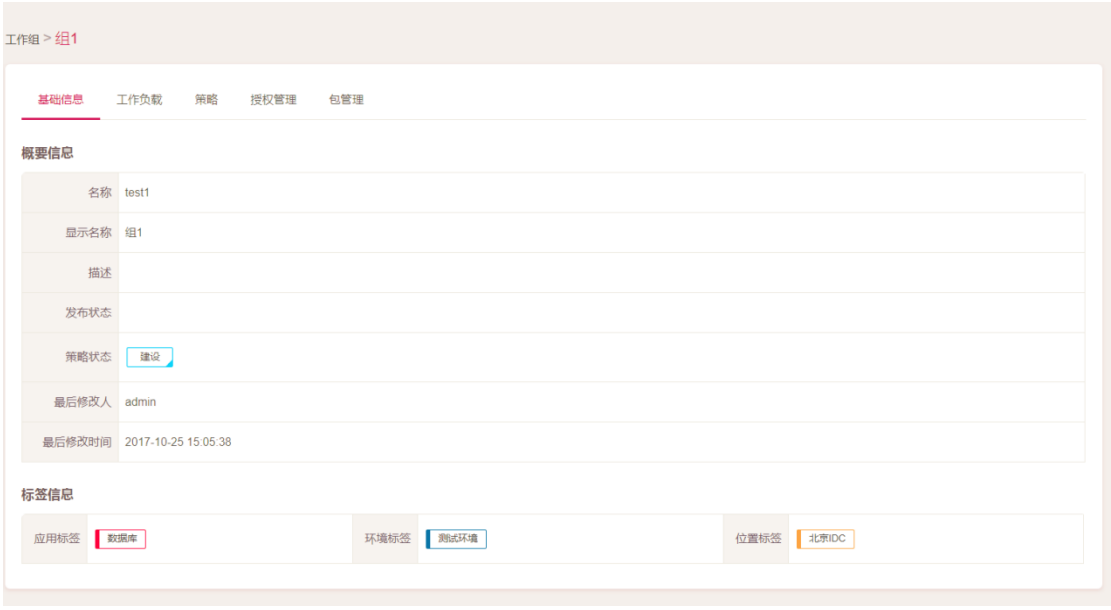
2.工作组页面右上方的搜索框可以对工作组进行过滤，页面中基本属性栏可以进行排序，  下箭头为正序，上箭头为反序。



3.点击 

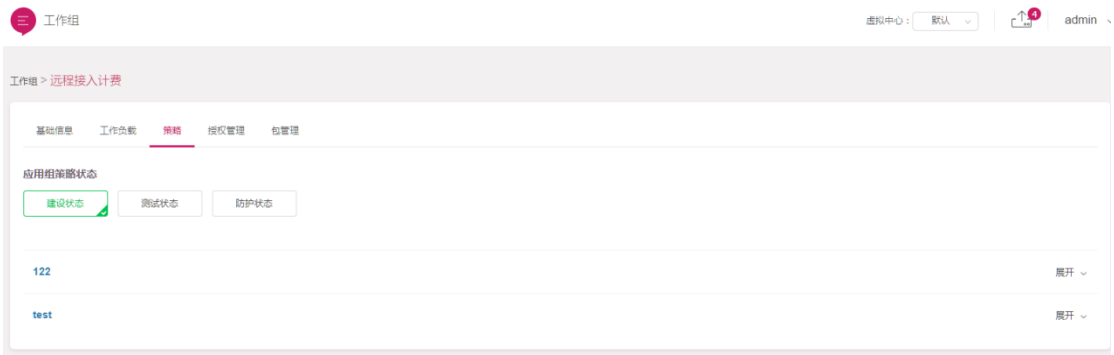
按钮，即可在弹出框中进行工作组的建立，一个工作组名称唯一，并选择 1-3 个标签。新建的工作组会出现在业务拓扑页面。

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。



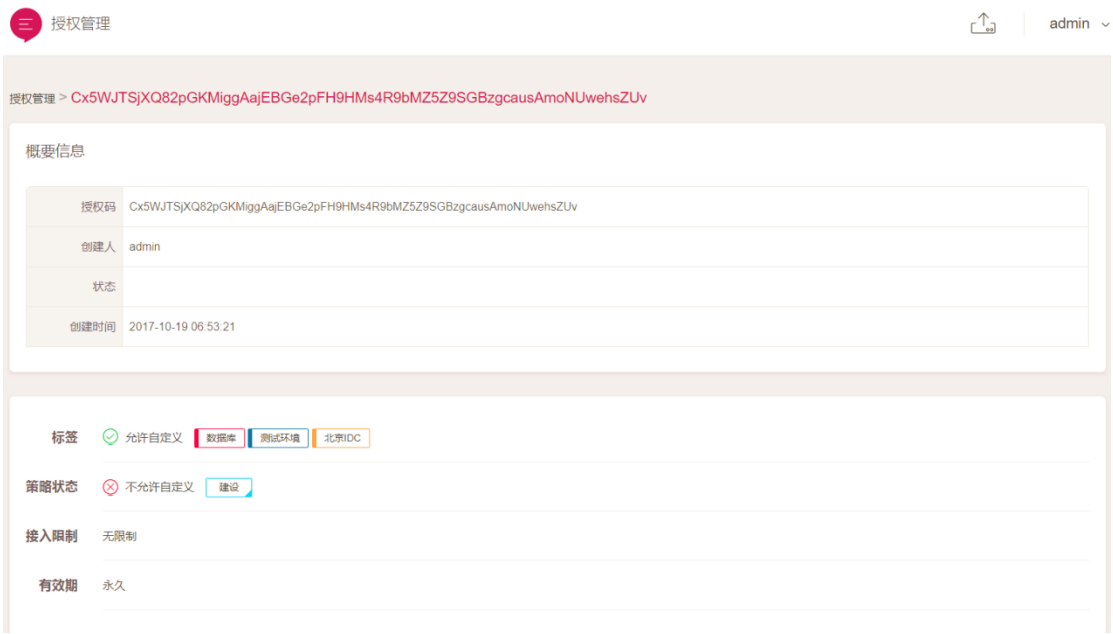
5.工作负载详情页面中的工作负载页面，可查看当前此工作组包含哪些工作负载，在此页面可批量将工作负载调整到外部，也可选择其他组的工作负载调整到本组。

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。



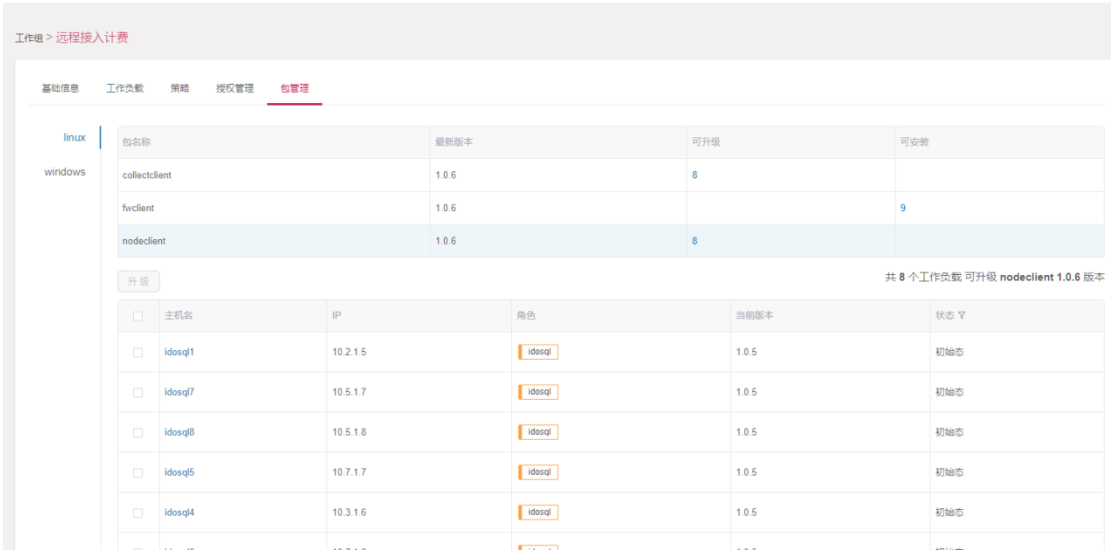
7. 工作负载详情页面中的策略页面，可查看与本工作组相关的授权码，即通过本授权码安装的工作负载，均自动位于该工作组。

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。

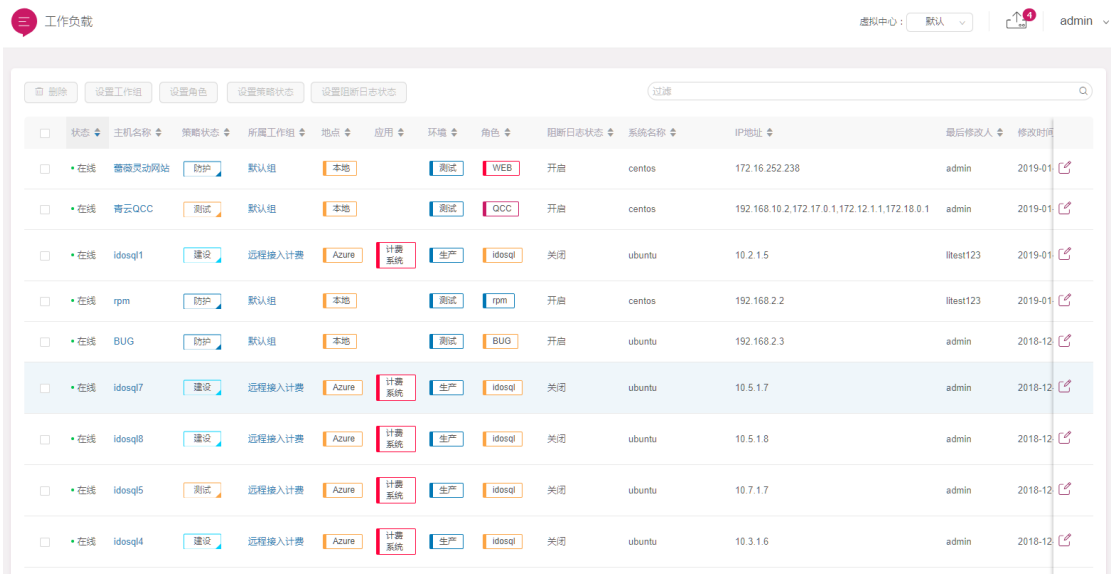


4.2.2 工作负载

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。

4.2.3 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。

4.3 安全策略管理模块

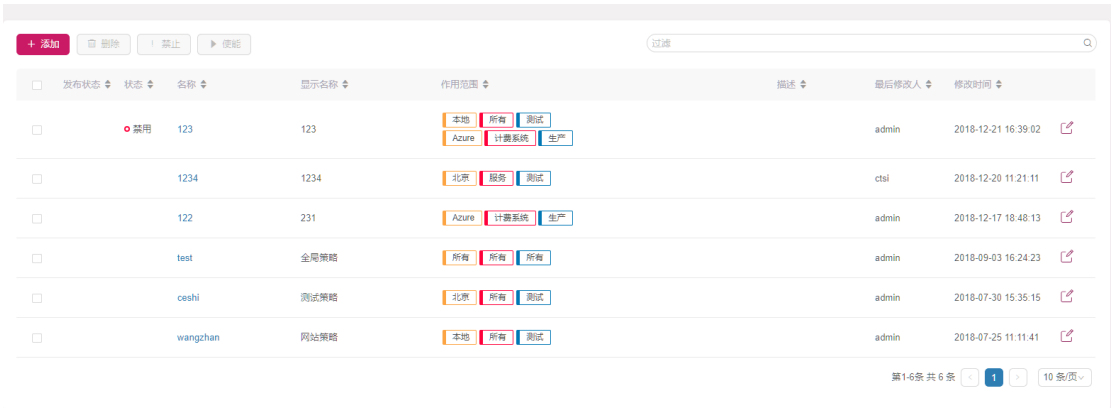
安全策略管理模块包括策略与策略集、服务对象、地址对象、更新发布、发布记录。服务对象、地址对象子模块主要为策略与策略集的建立提供支撑。更新发布、发布记录用于策略的发布流程以及后续查看、回滚。

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。

4.3.1 策略与策略集

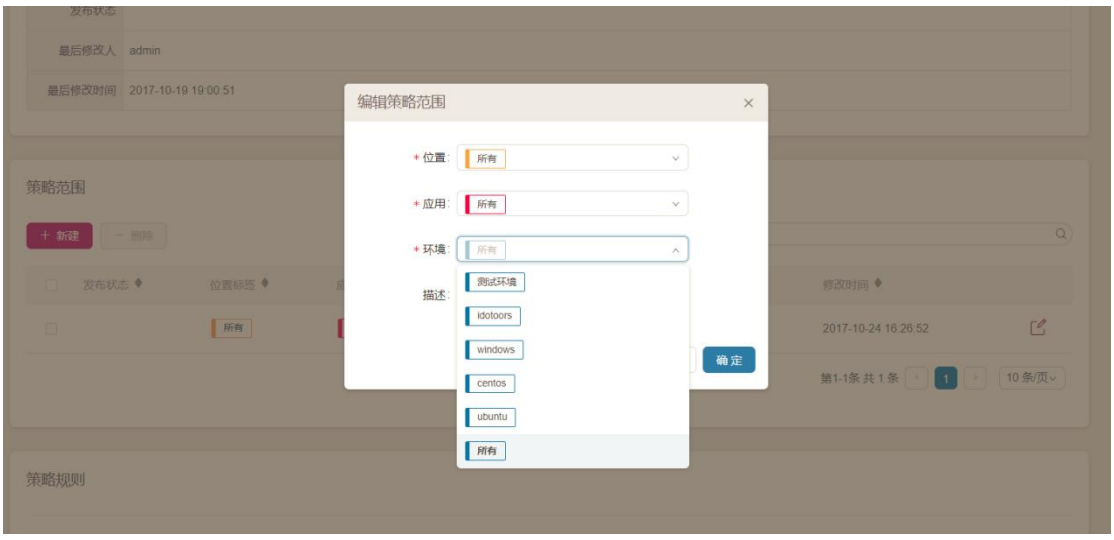
1.策略与策略集用于策略的建立、修改、删除、禁止与使能。可通过页面的搜索框进行过滤；每条策略最右侧的 图标用于修改该条策略的基本信息。界面如下：



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。

4.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。

4.3.2 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。

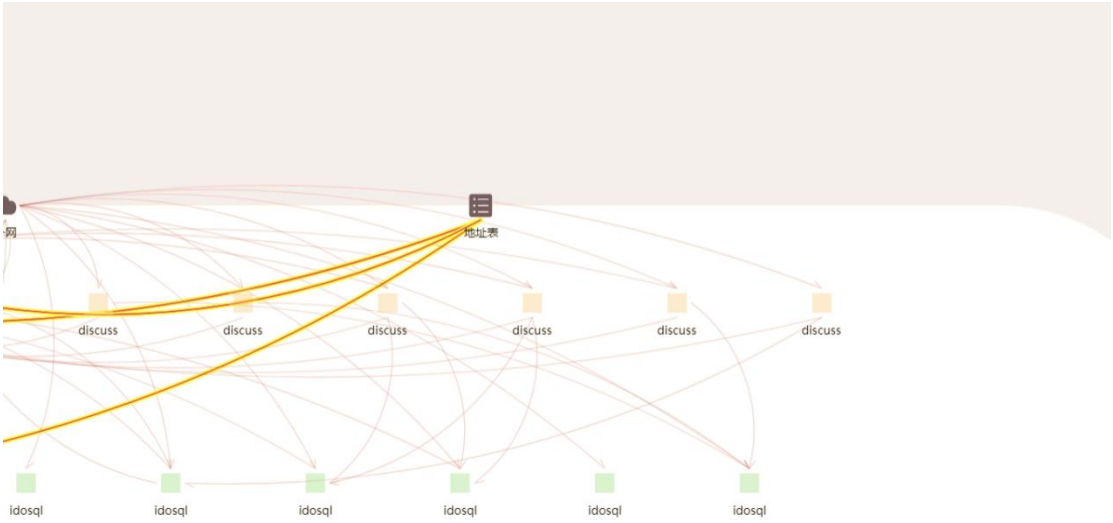
4.点击 

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。

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。

4.3.3 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。

4.点击 

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。

5.勾选对应的地址对象，点击 

按钮，可进行删除操作。

4.3.4 更新发布

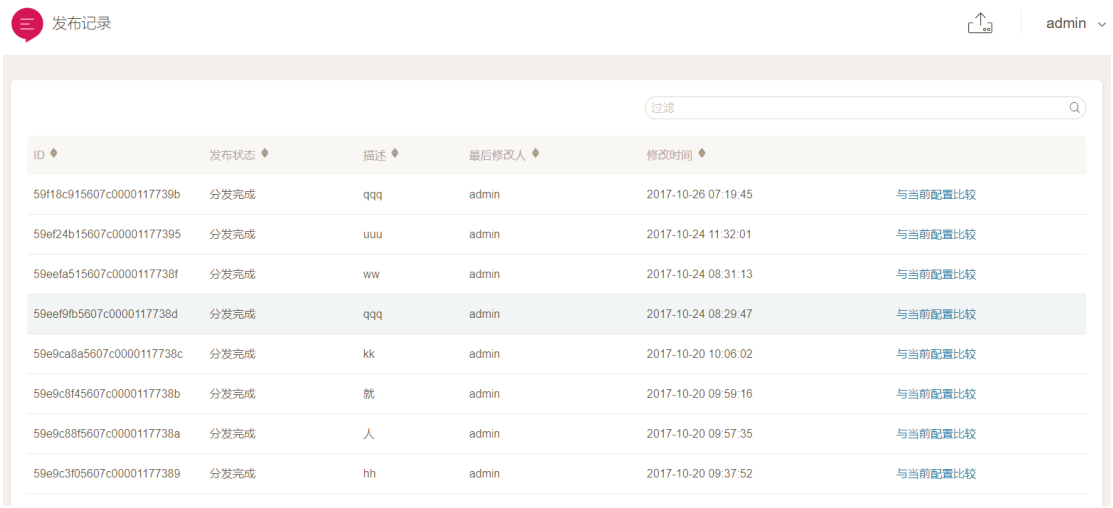
更新发布有两个作用，一是可以记录本次需要发布的所有操作，便于审阅；二是通过本页面点击发布，将本次的所有操作同步到 Agent。

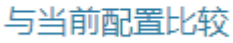
2.点击 

按钮，可将本次还未发布的操作进行还原。

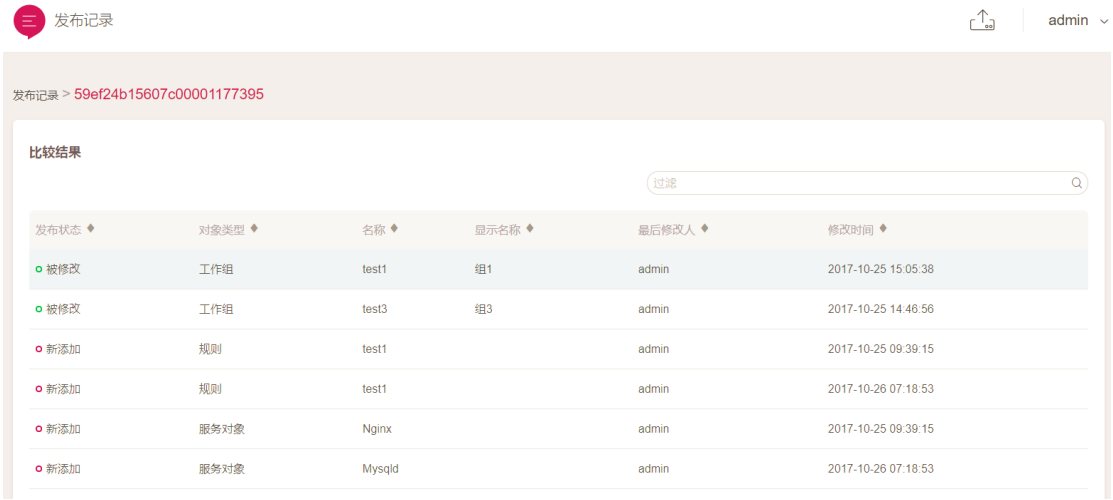
4.3.5 发布记录

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。



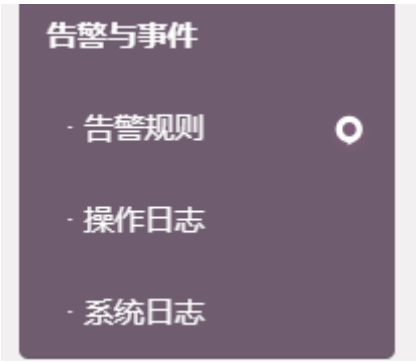


2.点击每条发布记录最右侧的 ，即可进入比较页面，本页面会显示本条发布记录时与现有策略的差别项。



4.4 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。



4.4.1 告警规则

进入告警规则界面后，可配置告警相关信息（邮件服务器地址需超级管理员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。

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。

4.4.2 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。

4.4.3 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。

4.5 排查工具

4.5.1 策略检查

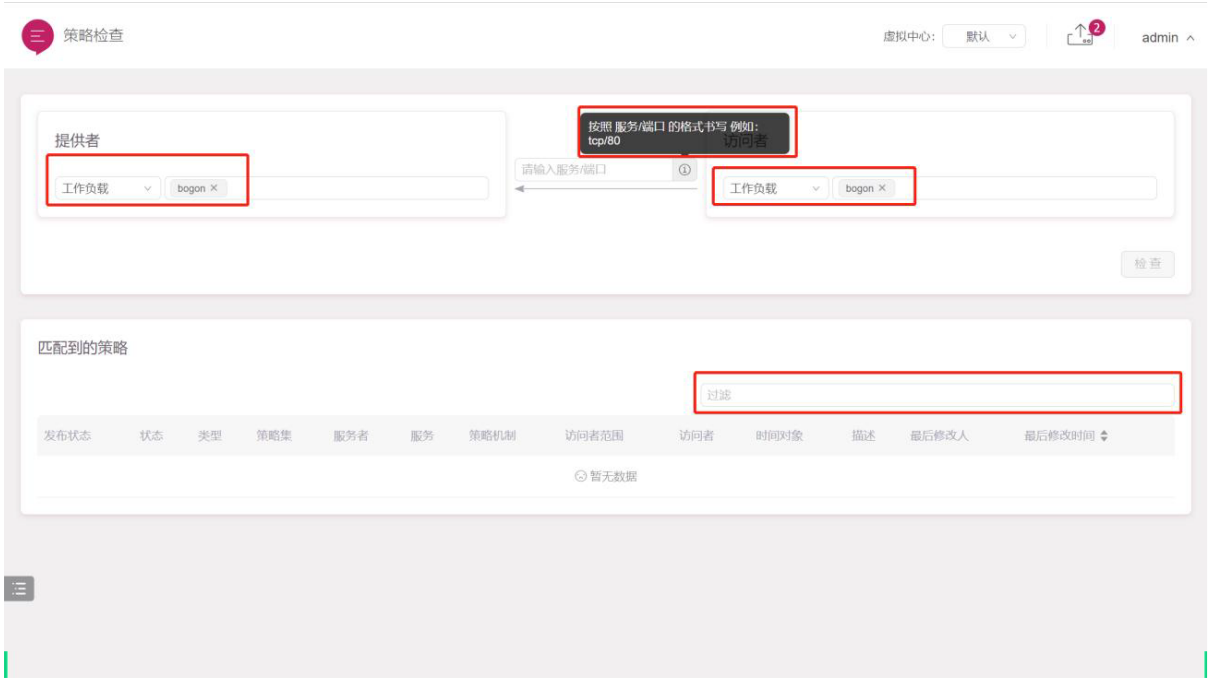
点击功能菜单->查询搜索->策略检查，进入此功能界面。

策略检查主要用于两个工作负载之间的通信服务端口进行策略匹配度检测，也可以用策略检查来去掉工作负载间的重复策略。

注意：只有匹配好的策略可以搜索到，没有匹配的，策略无法检查到。

在检查策略时，提供者和访问者需要提前选择，服务端口也需要提前填写好，否则无法检查。提供者和访问者在选择时也可以选择具体 IP，在检查结果过多的时候，可以通过过滤来检查想要的结果。

注意：提供者、访问者和服务端口都是单项填选。



4.5.2 连接关系

点击功能菜单->查询搜索->连接关系，进入此功能界面。

1.连接关系搜索用于查询工作负载的访问和被访问的详细情况，搜索结果数据支持导出查看。

2.在连接搜索界面中，端口服务是单项填写，本端和远端都是可以多项选择也可以不选择。在搜索时，可以添加搜索条件来获取相应的结果。在检查结果过多时，可以通过过滤来查看想要的结果。连接关系支持导出到本地进行查看。

4.5.3 阻断关系

点击功能菜单->查询搜索->阻断关系，进入此功能界面。

1.此功能用于查看本段和远端之间的阻断或者预阻断的详细信息，详细的阻断信息可以支持导出查看。

2.在阻断搜索界面中，本端和远端都是可以多项选择的。本端只能选择已安装客户端的工作负载，远端可选择工作负载或者 IP，可以时非安装客户端的 IP，下面可选择单向或者双向进行搜索。

4.6 系统配置

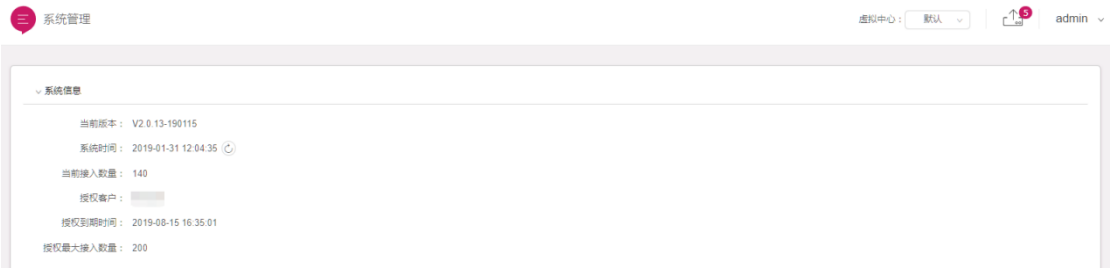
4.6.1 系统管理

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。

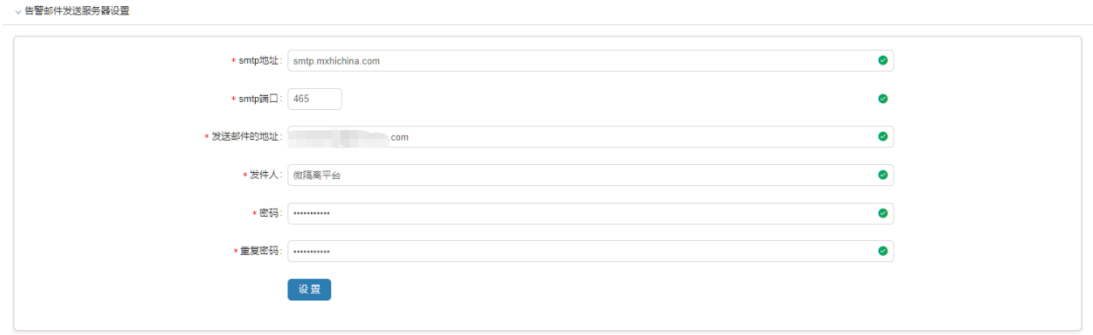
系统信息：包含系统版本、系统时间、license 数量、授权时间、客户名称等信息。



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。

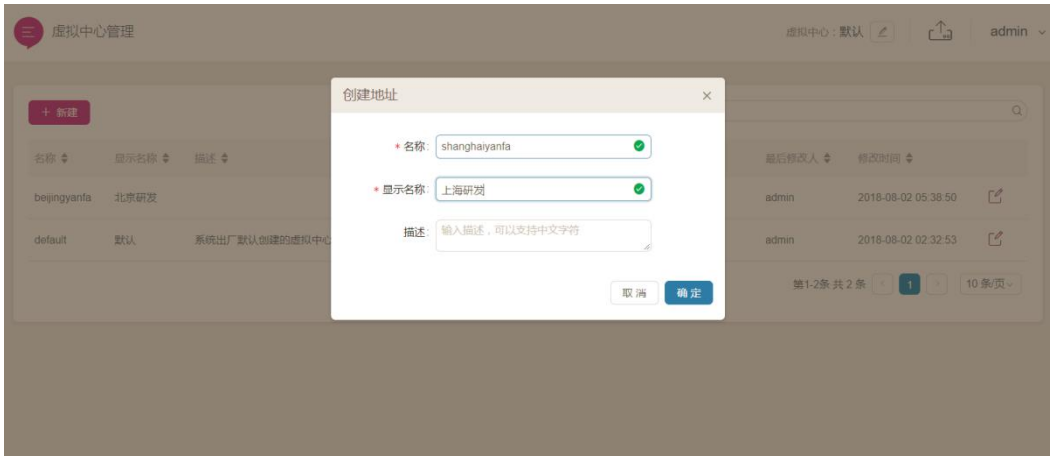
2)已接入数量达到授权数量后，接入新工作负载将失败。

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，需超级管理员用户根据内部实际情况先配置邮件发送服务器地址。



4.6.2 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：超级管理员可以看到所有虚拟空间。

4.6.3 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：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。

4.超级管理员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。

5 常见问题

5.1 售前类

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: 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:

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

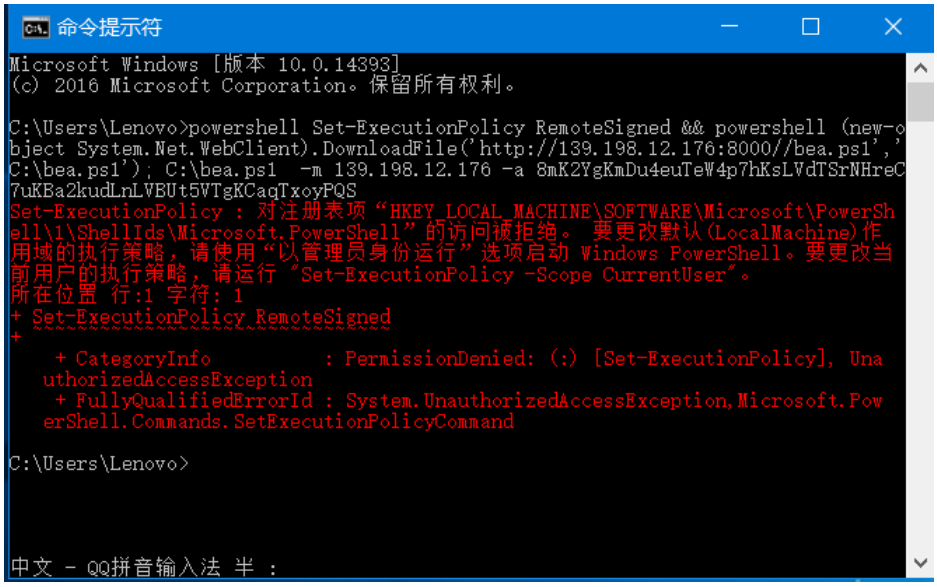
Windows 支持环境：Windows Server 2008 R2、2012、2012 R2、2016。(注：以上各版本 64 位系统) Windows7、10

Q: 业务拓扑图的红色线和绿色线都代表什么?

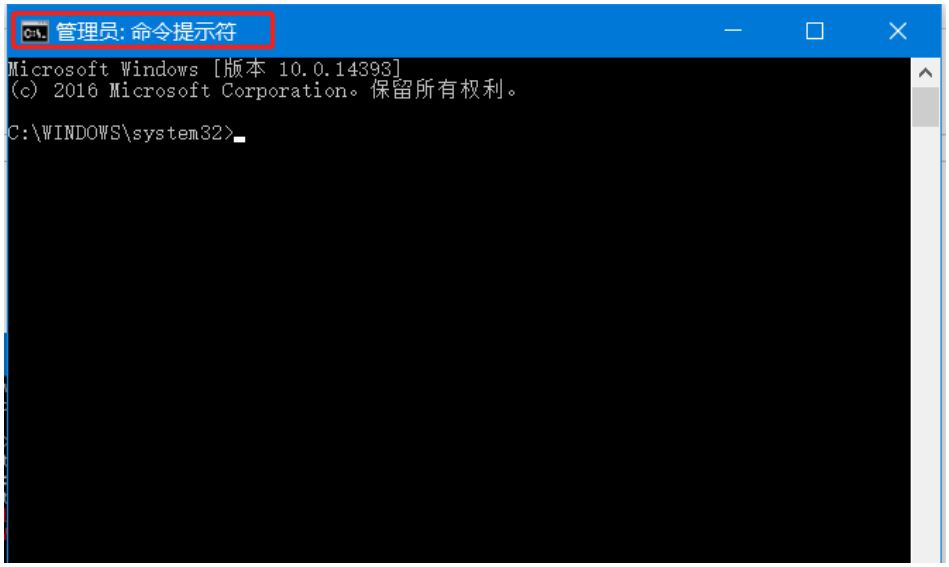
A: 业务拓扑图上的红色线代表工作负载被访问的流量连接与微隔离的策略没有匹配，当工作负载切换到防护，红色的流量连接将会被阻断；业务拓扑图上的绿色线代表工作负载访问的流量连接与微隔离的策略可以匹配上，当工作负载切换到防护，绿色的流量连接将会被放开允许访问。

5.2 操作类

Q:Windows 系统在安装客户端时，提示访问被拒绝，如下图所示:

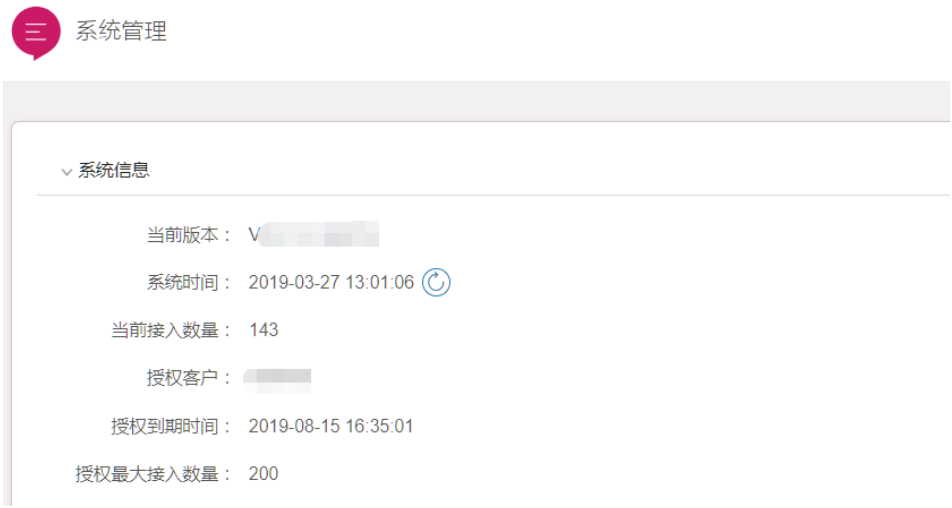


A：使用管理员权限运行 CMD，并执行安装命令。



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。



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，访问请忽略证书安全性要求，继续访问即可。

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位置查看“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?

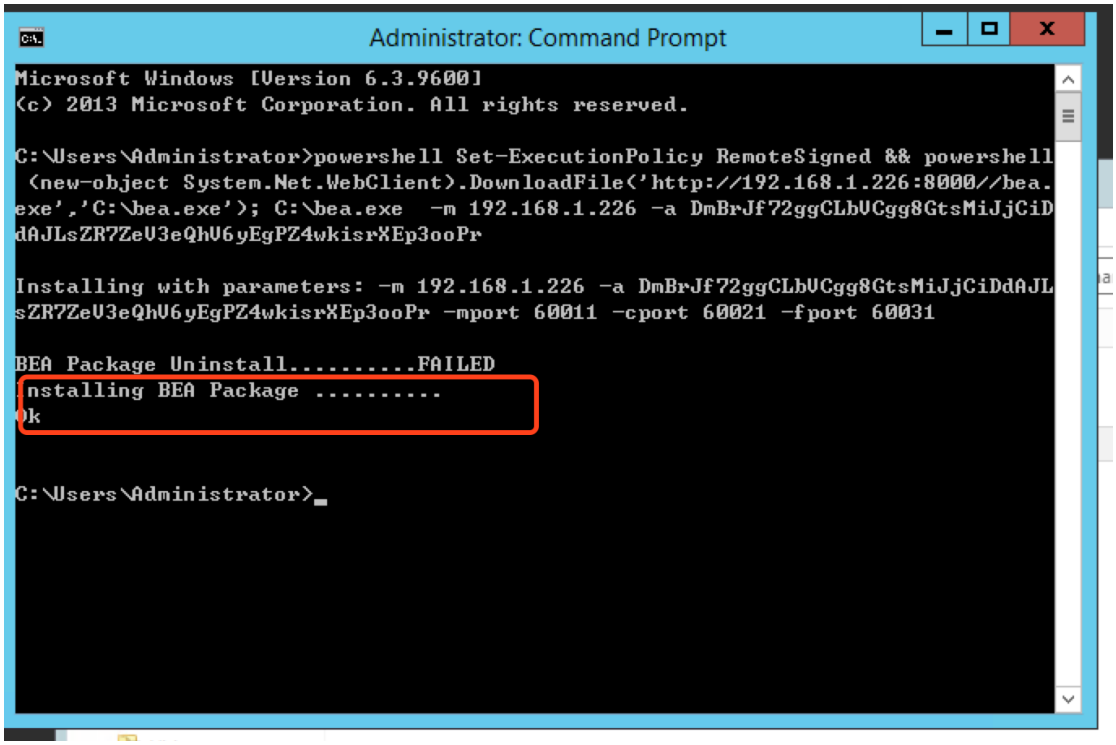
A: Linux 环境下安装过程提示 nodeclient、collectclient 和 fwclient 服务正常即安装成功，如下图

```
************************************************************
*                    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
```

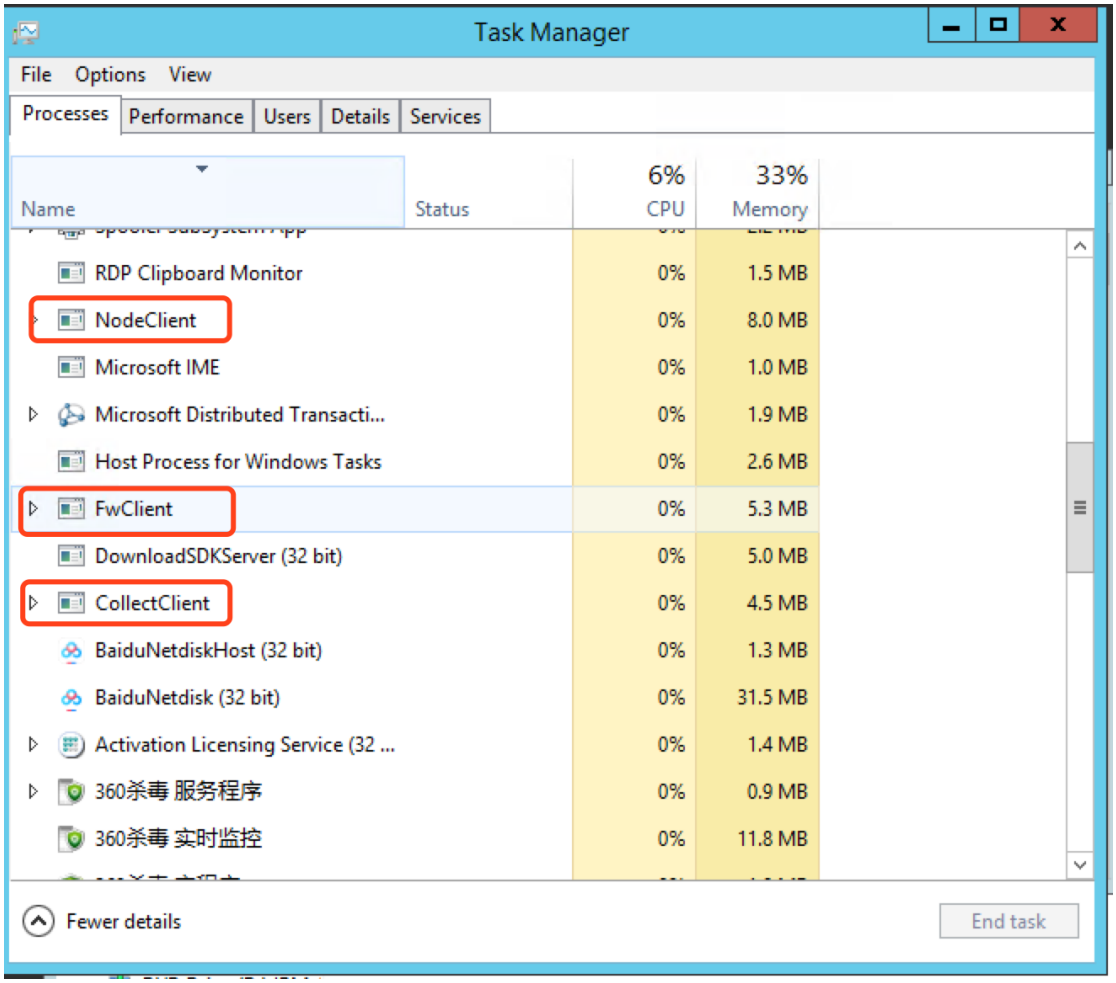
如果是安装一段时间后查看是否 agent 客户端工作正常，请使用 ps aux | grep client，如下图三个 client 正常存在即为正常

```
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。



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: 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

5.3 服务类

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: 请联系 400 客服获取。

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。