

蔷薇灵动自适应微隔离安全平台

V2.0 使用说明书



2018 年 6 月 10 日

内部资料，请勿外传

目录

蔷薇灵动自适应微隔离安全平台 V2.0 使用说明书	1
一、引言	3
1.1 编写目的	3
1.2 产品简介	3
1.3 产品架构	3
二、使用说明	4
2.1 登录及用户管理	4
2.2 系统管理	5
2.3 业务拓扑界面使用说明	6
2.3.1 首界面基本功能说明	6
2.3.2 拓扑使用说明	8
2.4 创建工作组	11
2.4.1 新建组标签	11
2.4.2 创建工作组	12
2.5 接入工作负载	13
2.5.1 创建授权码	13
2.5.2 接入工作负载	15
三、其他功能说明	15
3.1 工作负载管理模块	15
3.1.1 工作负载	16
3.1.2 标签管理	17
3.2 安全策略管理模块	18
3.2.1 策略与策略集	18
3.2.2 服务对象	21
3.2.3 地址对象	23
3.2.4 工作组	26
3.2.5 更新发布	31
3.2.6 发布记录	31
3.3 告警与事件	32

一、引言

1.1 编写目的

本说明书主要为用户展示蔷薇灵动蜂巢自适应安全平台 V2.0（以下简称自适应安全平台或平台）的主要功能及操作步骤。主要包括：登录及用户管理、客户端安装、业务拓扑的查看及操作说明、安全策略管理、工作负载管理、告警与事件的查看。希望用户能够通过阅读本使用说明，对自适应安全平台的功能有一定了解，并能结合对产品的操作，具备对产品的应用能力。

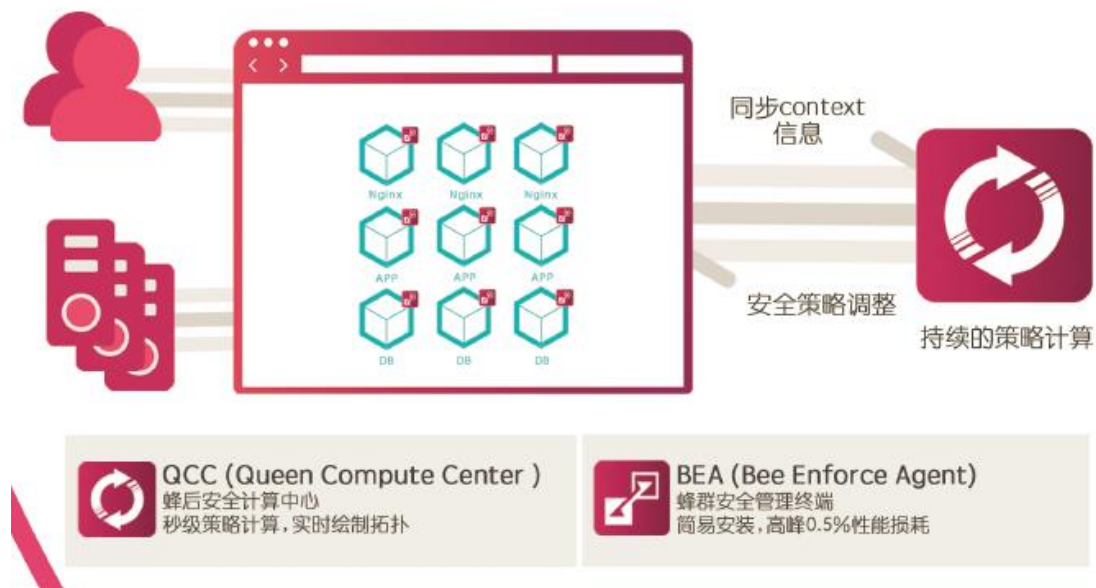
1.2 产品简介

蔷薇灵动蜂巢自适应安全平台是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，和细粒度的安全策略管理。能够帮助用户快速便捷地实现环境隔离、域间隔离以及端到端隔离。

产品基于完全自主开发的一套自适应安全架构，将安全能力与工作负载（workload）紧密结合起来，而不是在工作负载之外做安全，而且做到了与底层架构无关，使得产品在混合云统一安全管理，业务与安全同步交付，容器间安全等问题上具备了完美的解决能力。

1.3 产品架构


蔷薇灵动蜂巢自适应安全平台的总体技术架构由两部分组成，一部分是安装在主机上的蜂群安全管理终端 BEA（Bee Enforcement Agent），一部分是集成的蜂后安全计算中心 QCC（Queen Compute Center）。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

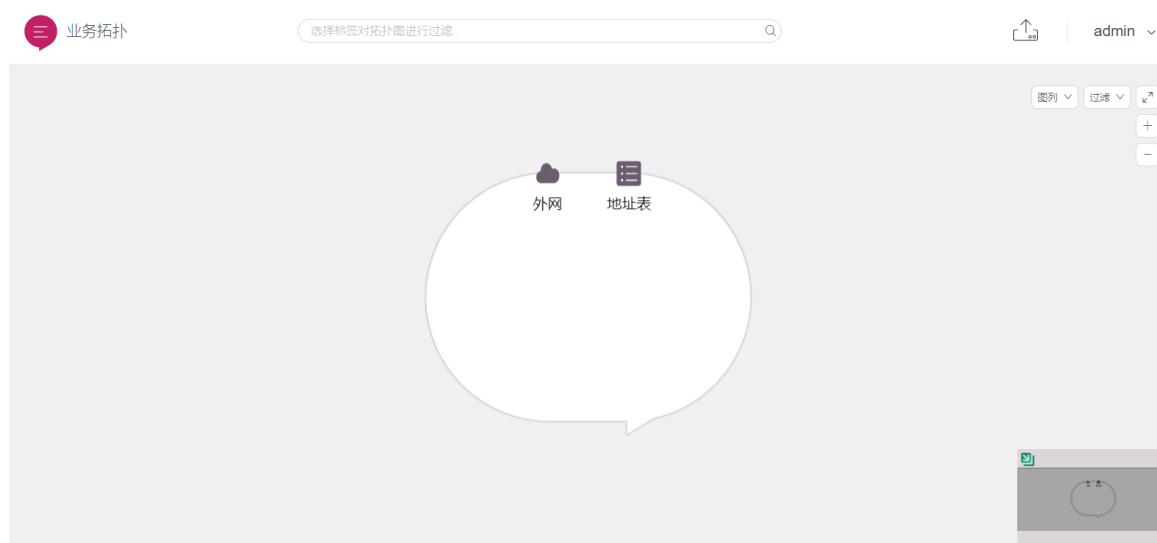
二、使用说明

2.1 登录及用户管理

1. 产品采用 web 页面进行管理 & 操作, 在浏览器输入 “https://+管理地址” 即可进入登录界面, 界面如下。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。



2. 登录完成，进入平台（V2.0）首界面，首次登录时，界面如下



3. 点击首界面右上角的用户名，即可进入用户管理界面，以及可退出当前用户。如下图所示：



4. 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。

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，但不能查看系统及操作日志。

审查员：只可以查看及操作系统及操作日志。

2.2 系统管理

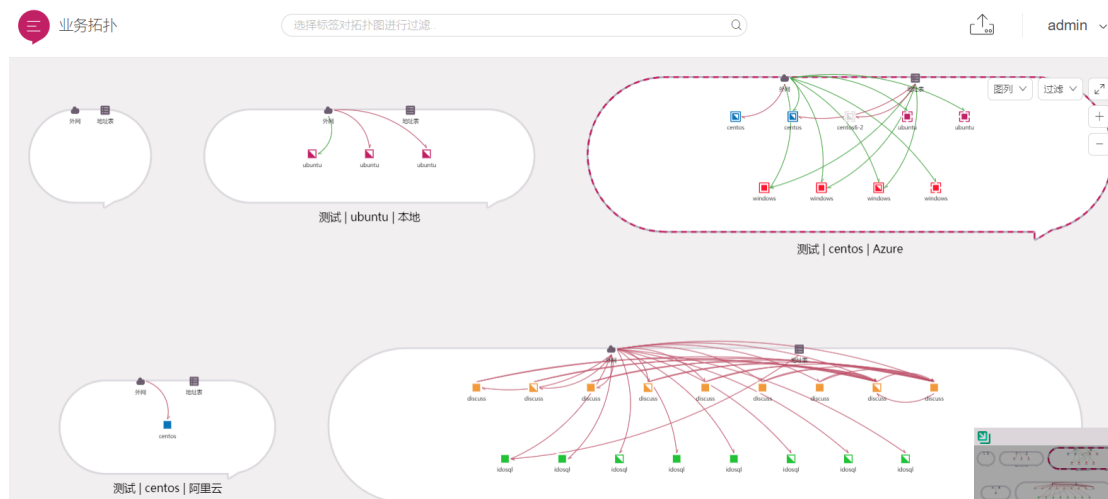
系统管理可设置系统相关参数，包括日志储存天数、登录尝试次数、会话时长等。还可解锁其他被锁定账户。


只有超级管理员具备进入系统管理的权限。

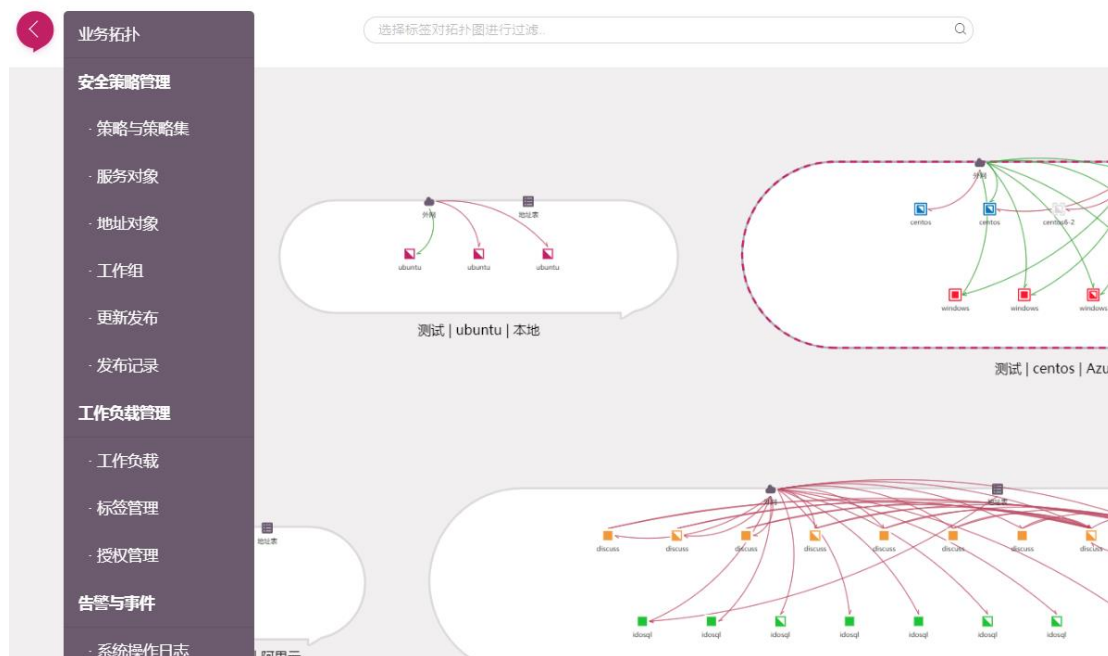
2.3业务拓扑界面使用说明

2.3.1 首界面基本功能说明

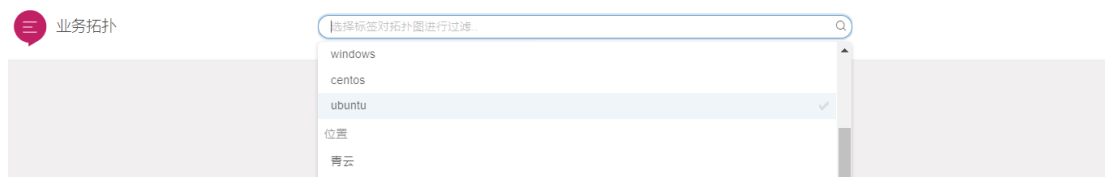
1. 为了更好的展示及说明业务拓扑的功能及操作，以下使用已包含多台工作负载的自适应安全平台进行说明。Demo 界面如下：





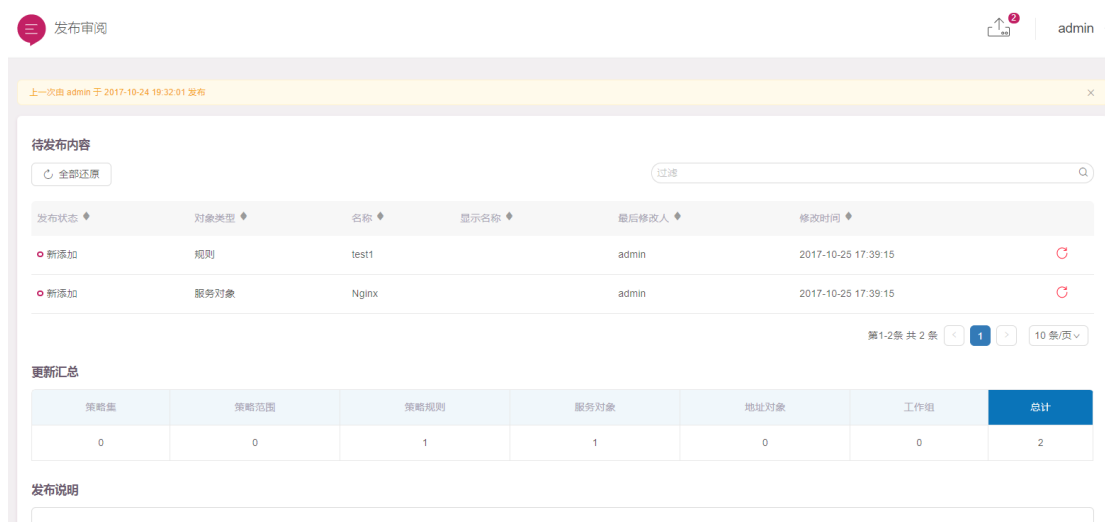
2. 页面左上角的  标识，点击后会弹出自适应安全平台功能列表，如下图所示，点击各功能标签可进入各功能页面。



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。




4. 界面右侧的  标志，为发布提示标志，当平台的某些操作需要同步到工作负载时，该图标会显示需要同步的数量 。点击该图标可进入发布审阅界面。






5. 首界面拓扑左上角的图例  标志，点击后可查看业务拓扑界面元素说明。



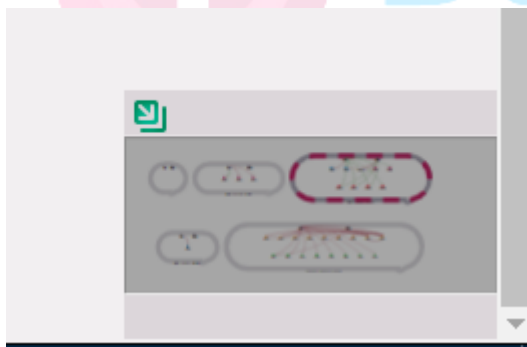
6. 图例标识右侧的过滤  标识，点击后，可对拓扑中的连接线进行过滤，分为忽略业务组间流量、忽略指定服务、忽略低访问量业务、忽略不活跃业务，

如下图所示：



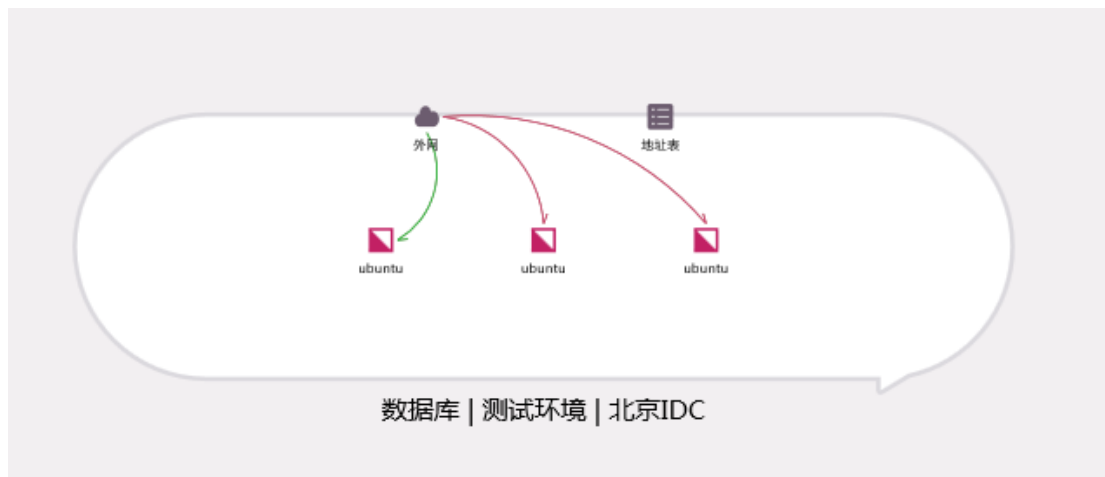
7. 最右侧的  标识可对界面进行全屏展示， 以及  标识可以放大或缩小拓扑。

8. 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。



2.3.2 拓扑使用说明

1. 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。
2. 工作组中每个小方块代表一个工作负载，。



3. 拓扑中每条连接线均代表此元素对于工作负载的访问链接，拓扑中的元素包括外网、地址表、工作负载。双击连接线，可查看该元素与此工作负载的所有链接。

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]

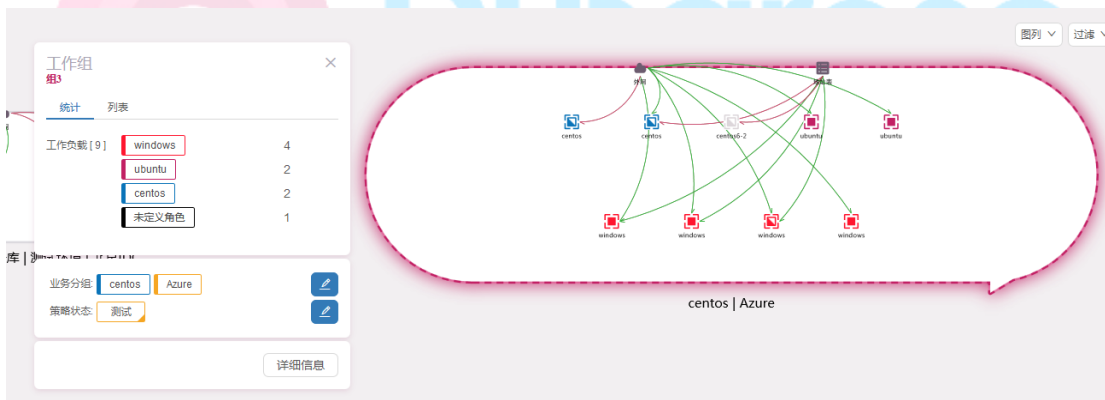
101.230.198.136	103.27.238.213	104.131.124.154
106.120.40.28	106.39.39.18	106.39.39.28
106.75.63.218	109.195.86.75	109.195.94.50
111.127.118.22	111.40.120.33	113.113.120.243
113.95.40.150	114.114.120.50	114.114.120.110

重新统计 查看策略 ▾

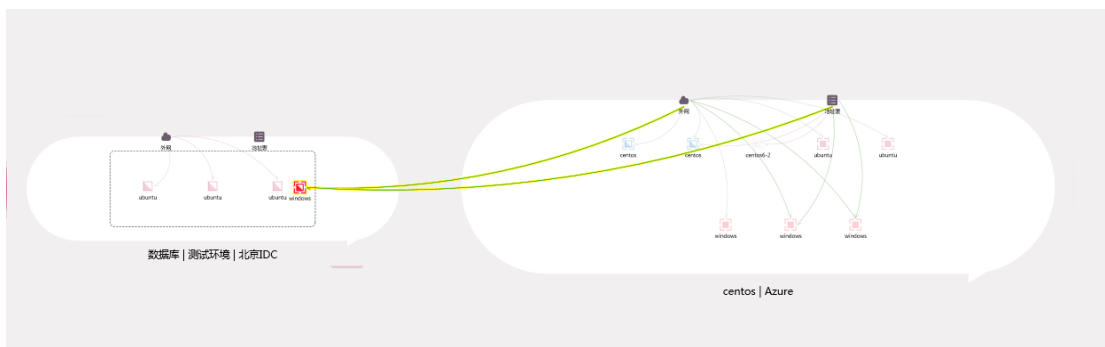
4. 双击工作负载图标可查看此工作负载的基本信息。



5. 双击工作组，可查看工作组的基本信息。



6. 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。另外对于工作负载在组间的移动时，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。



2.4 创建工作组

在接入工作负载之前，推荐可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）。

2.4.1 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）。



3. 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。



2.4.2 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，标签选择事先创建的。每个工作组由 1-3 个组标签定义，若某一项无标签，可选择空。



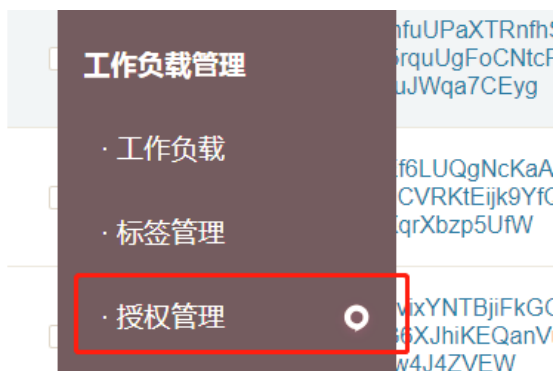
3. 点击确定后，工作组建立完成，拓扑图中会出现该工作组。

2.5 接入工作负载

2.5.1 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。

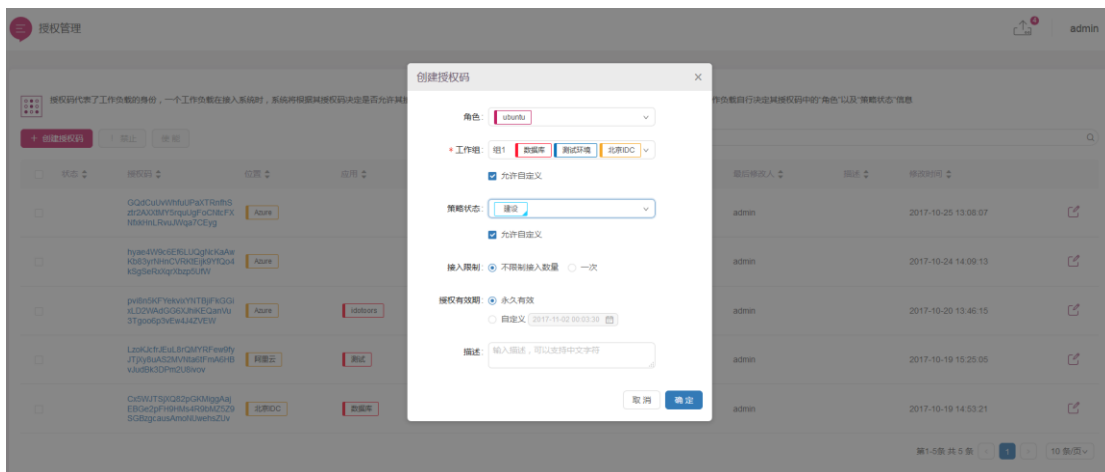


第二个入口，可以通过工作组详情查看该工作组的授权码（由某个组的授权码接入的工作负载，将自动分配到该工作组）。



2. 创建授权码

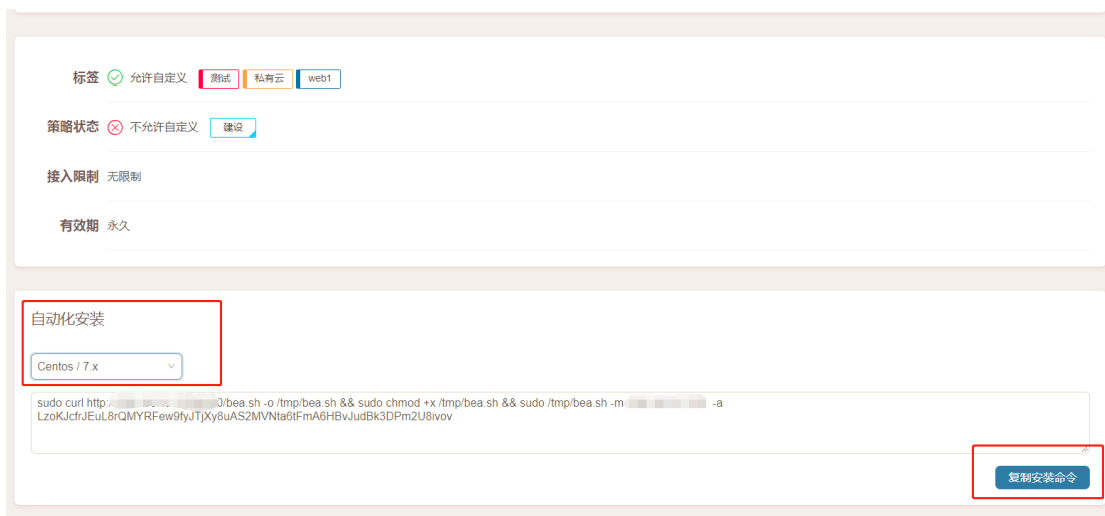
点击创建授权码，在弹出的对话框中输入相关参数。点击确定即可完成授权码的建立。



2. 点击授权码，可进入授权码详细页面。

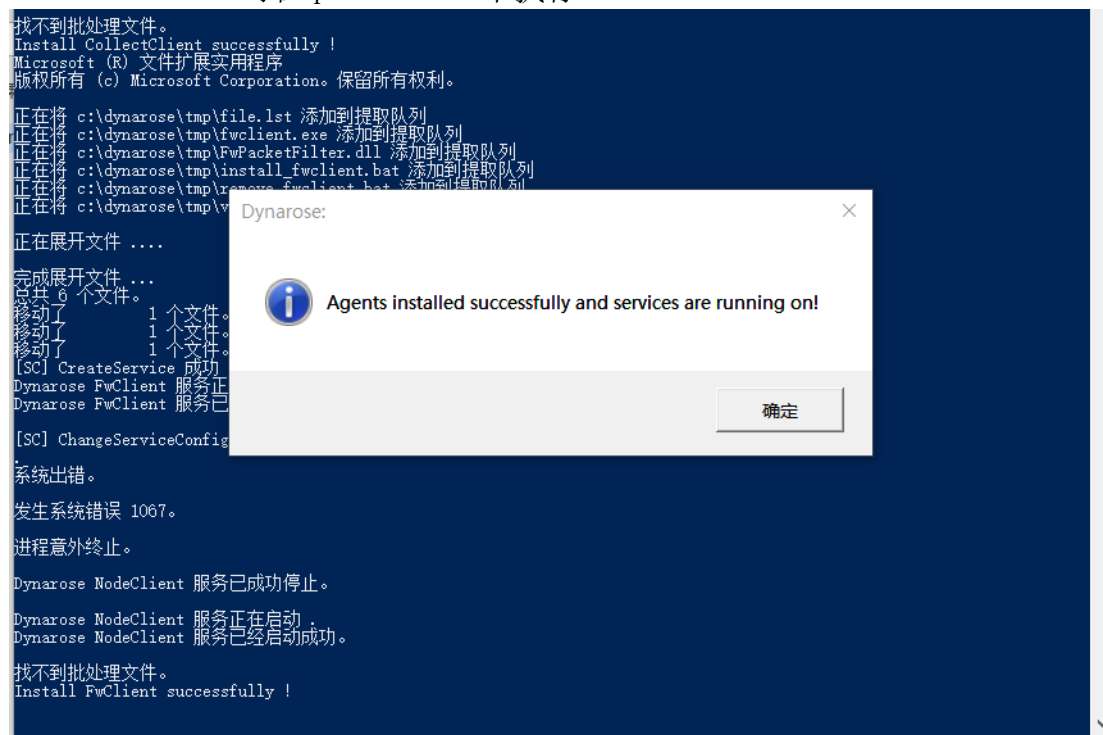


3. 授权码详细页面最下方的自动化安装部分，可根据此授权码自动生成安装命令，用于实现工作负载的自动化安装。



2.5.2 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 powershell 中执行。

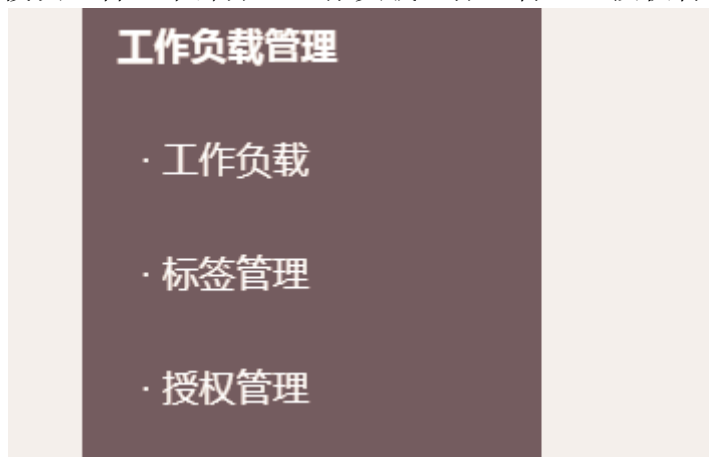


也可以使用自动化运维工具进行批量安装。

三、其他功能说明

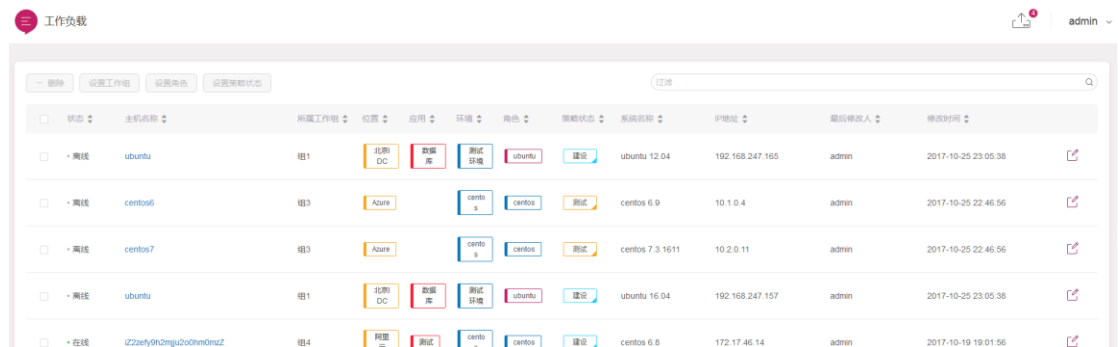
3.1 工作负载管理模块

工作负载管理模块包含三个部分：工作负载、标签管理、授权管理

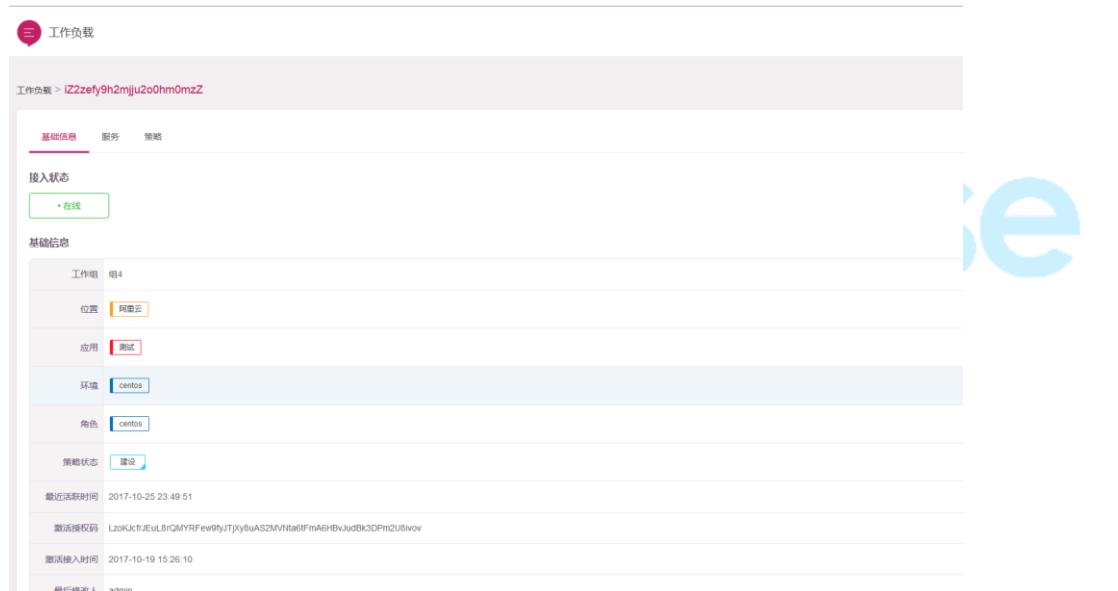


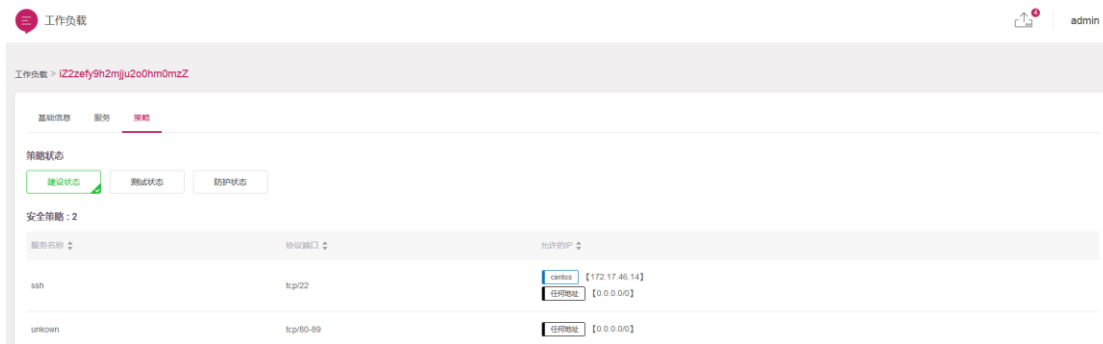
3.1.1 工作负载

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。



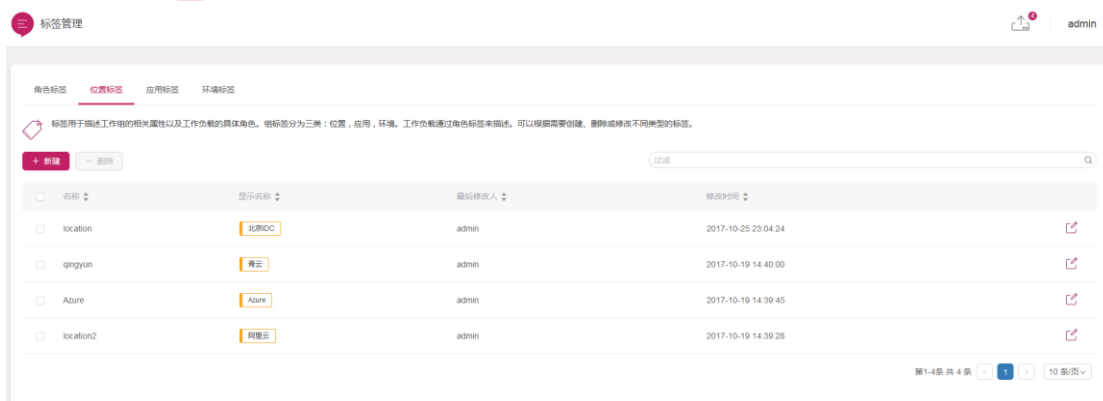
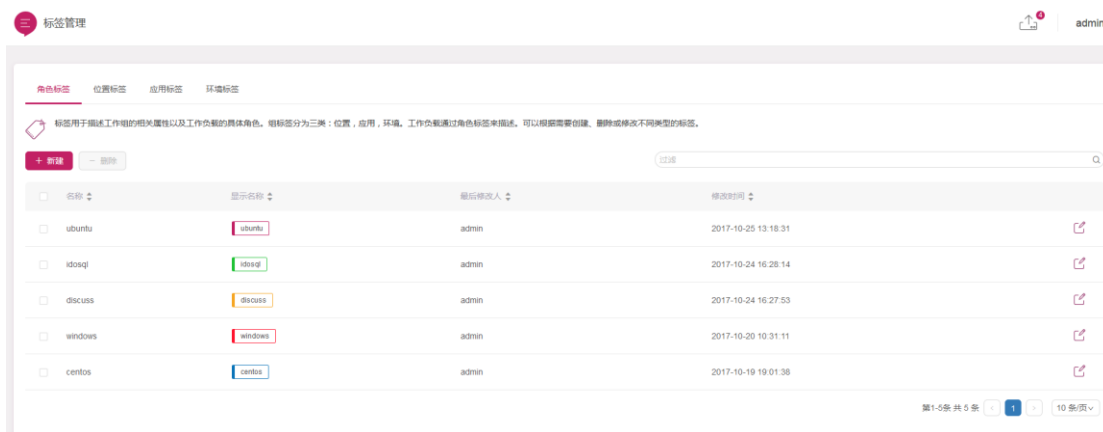
2. 点击工作负载的主机名称，可进入该工作负载的详细信息页面，包括其基本信息、服务信息、策略信息。





3.1.2 标签管理

1. 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。工作负载通过角色标签来描述。可以根据需要创建、删除或修改不同类型的标签。



2. 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。




3. 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。

3.2 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、工作组、更新发布、发布记录。服务对象、地址对象、工作组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。

3.2.1 策略与策略集

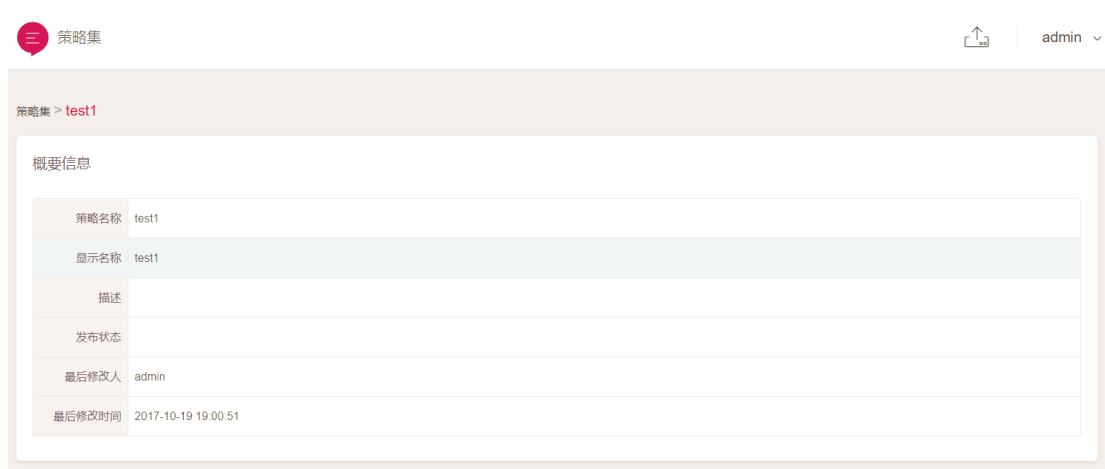
1. 策略与策略集用于策略的建立、修改、删除、禁止与使能。可通过页面的搜索框进行过滤；每条策略最右侧的  图标用于修改该条策略的基本信息。界面如下：



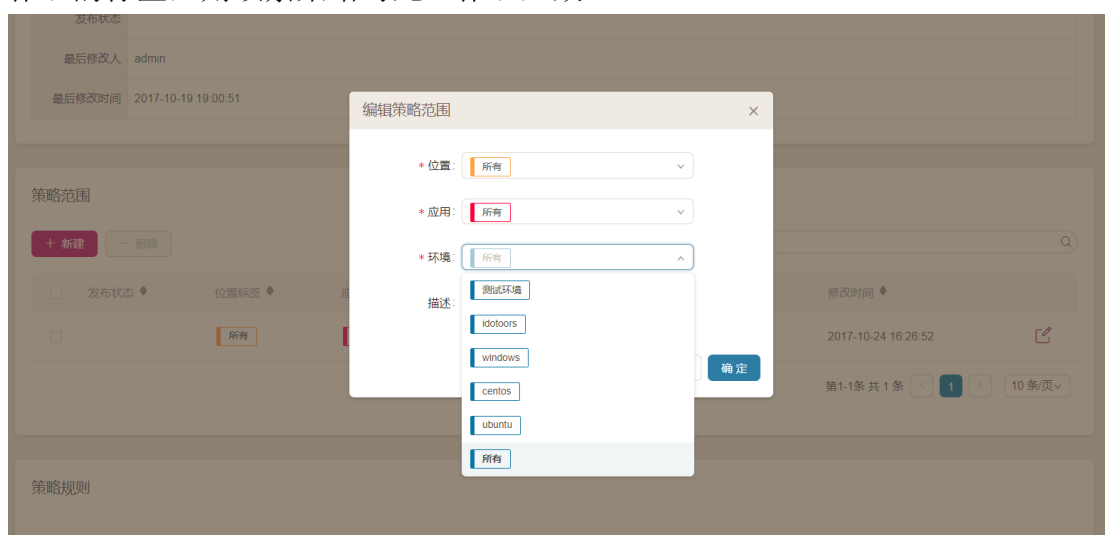
2. 点击添加，在弹出框内输入名称等信息，即可新建一条策略。



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，策略分为组间策略与组内策略。

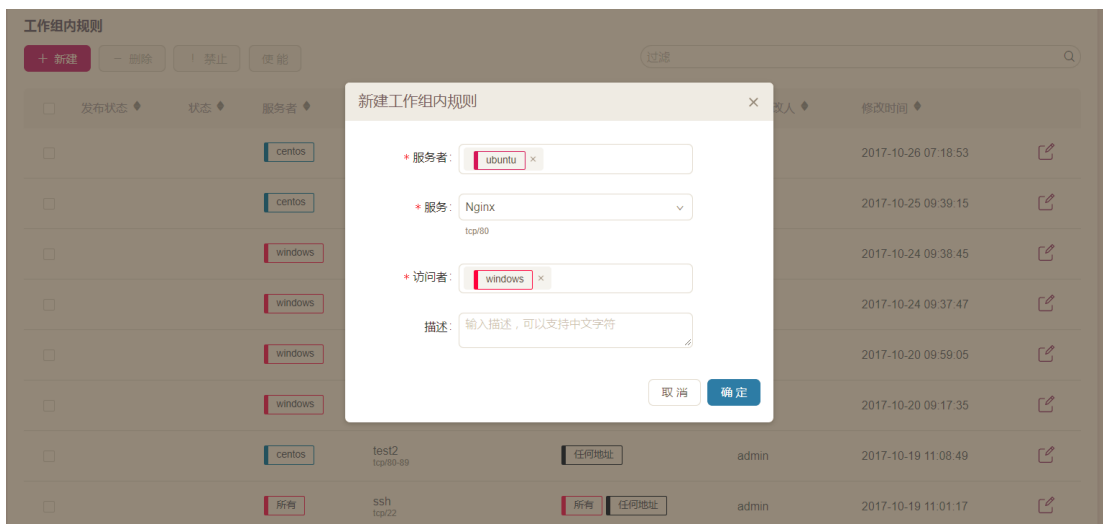



4. 策略范围是通过选择工作组标签来设定的，若策略范围所选定的标签涵盖某工作组的标签，则该条策略对此工作组生效。



5. 策略规则分为组内规则和组间规则，分为作用于策略范围所涵盖的工作组内和这些组与组之间的访问。在工作组内规则内点击新建，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。（注：只有已建立角色的工作负载才可被选择，服务对象也需事先确定）

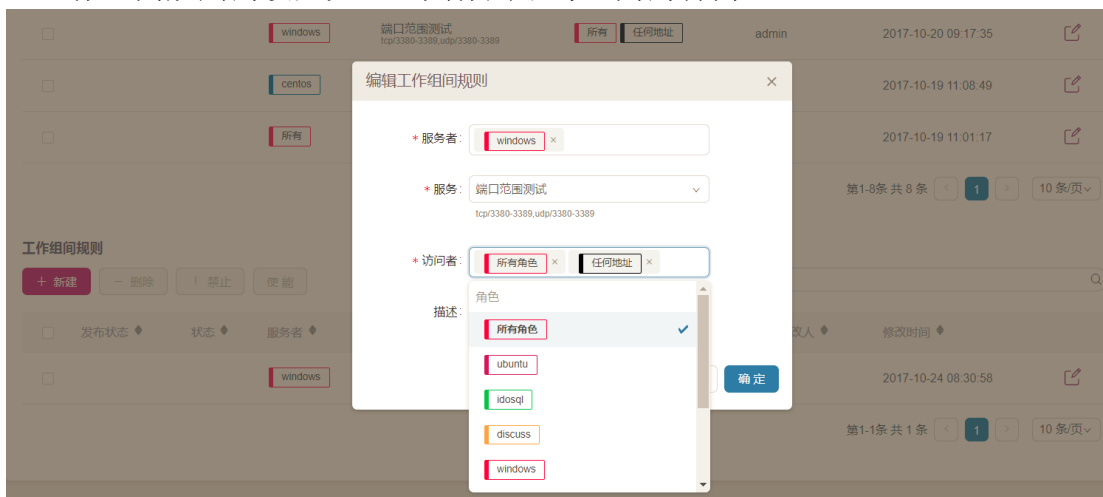
例如，我们让标签为 windows 的工作负载可以访问标签为 ubuntu 的工作负载的 Nginx (tcp/80) 服务，具体设置如下图：



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，其作用于跨组间的访问。



3.2.2 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。




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。



3. 点击 **+ 添加** 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。



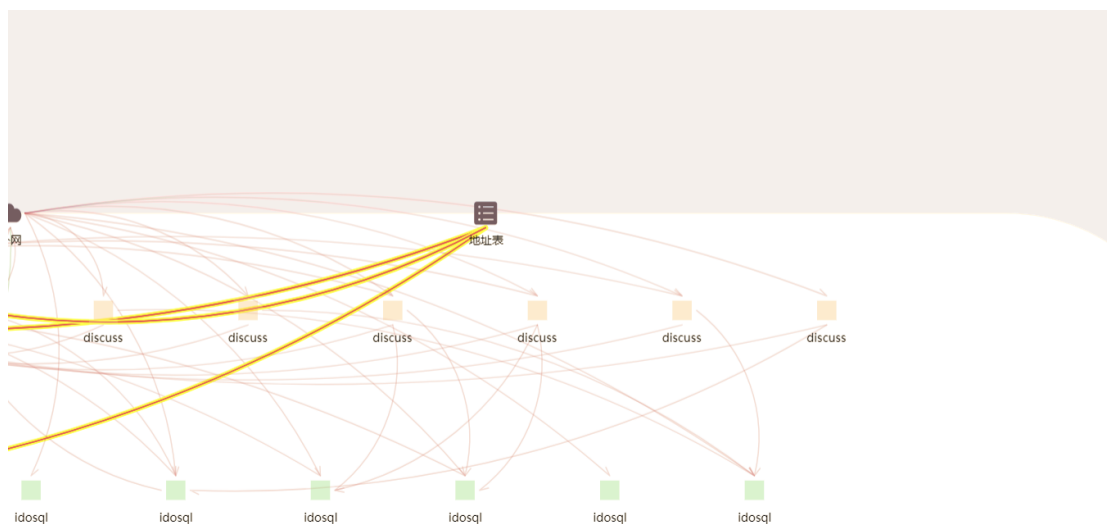
4. 点击每条服务对象最右侧的  标识可对服务对象进行修改，名称不可修改。可修改显示名称及服务的协议端口。

蔷薇灵动

名称	服务	描述	最后修改人
编辑服务 ✕			
名称:	<input type="text" value="svchost.exe"/>		
* 显示名称:	<input type="text" value="输入显示名称, 可以支持中文字符"/>		
* 服务 (?):	<input type="text" value="tcp/3389"/>		
描述:	<input type="text" value="输入描述, 可以支持中文字符"/>		
		<input type="button" value="取消"/>	<input type="button" value="确定"/>

3.2.3 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。

编辑地址 ✕

名称:

* 显示名称:

* 地址掩码 [?]:

描述:

5. 勾选对应的地址对象，点击

删除

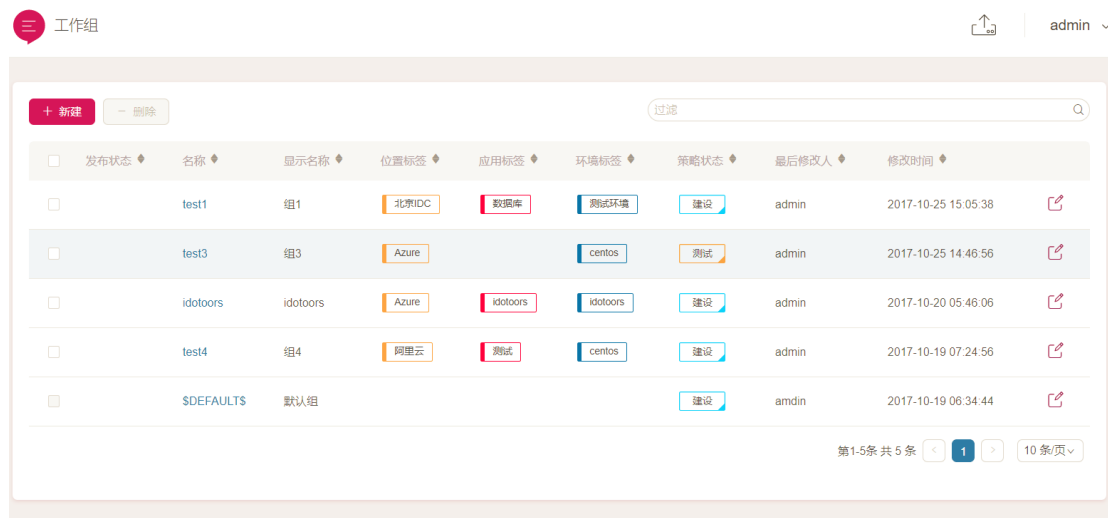
按钮，可进行删除操作。

地址对象

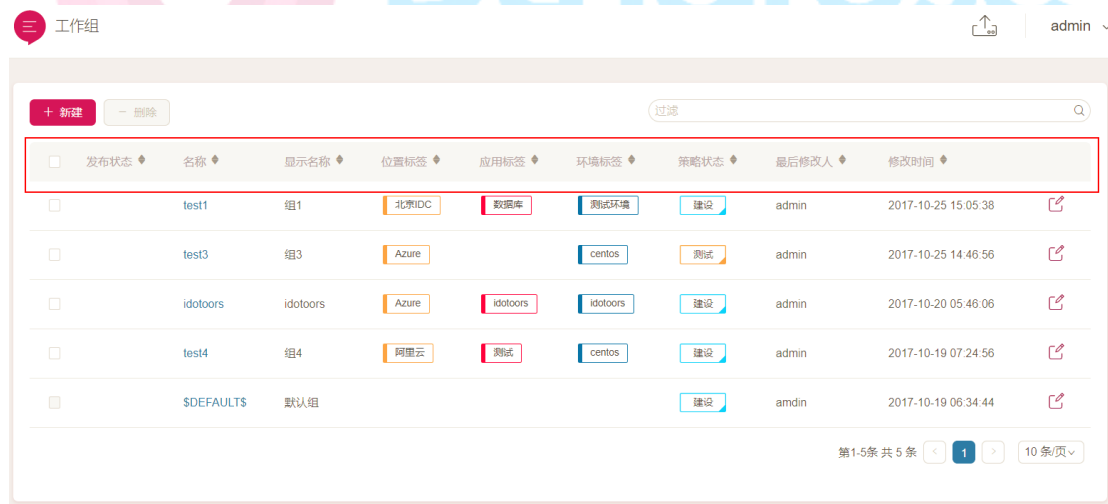
<input checked="" type="checkbox"/>	发布状态	名称	显示名称	地址与掩码
<input checked="" type="checkbox"/>		test	本地管理ip	124.202.184.186/32,218.241.251.151/32
<input type="checkbox"/>		ANY	任何地址	0.0.0.0/0

3.2.4 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 **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。

新建工作组

* 名称: 输入标签名称, 仅支持大小写英文字符

* 显示名称: 输入标签的显示名称, 可以支持中文字符

* 位置标签: 选择或筛选位置标签

* 应用标签: 选择或筛选应用标签

* 环境标签: 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

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。

工作组 > 组1

基础信息 工作负载 策略 授权管理 包管理

组1

主机名	IP地址	角色标签
ubuntu	192.168.247.165	ubuntu
ubuntu	192.168.247.157	ubuntu
ubuntu14	192.168.247.168	ubuntu

组3

主机名	IP地址	角色标签
centos6	10.1.0.4	centos
centos7	10.2.0.11	centos
centos6-2	10.1.0.5	
windows2012r2-2	10.1.1.7	windows
windows2008-2	10.1.1.6	windows

基础信息 工作负载 策略 授权管理 包管理

组1

主机名	IP地址	角色标签
ubuntu	192.168.247.165	ubuntu
ubuntu	192.168.247.157	ubuntu
ubuntu14	192.168.247.168	ubuntu

组3

主机名	IP地址	角色标签
windows2008-2	10.1.1.6	windows
windows2016-3	10.1.1.9	windows
ubuntu14	10.1.2.4	ubuntu
ubuntu16	10.0.0.4	ubuntu
windows2012r2-2	10.1.1.7	windows

6. 工作负载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。

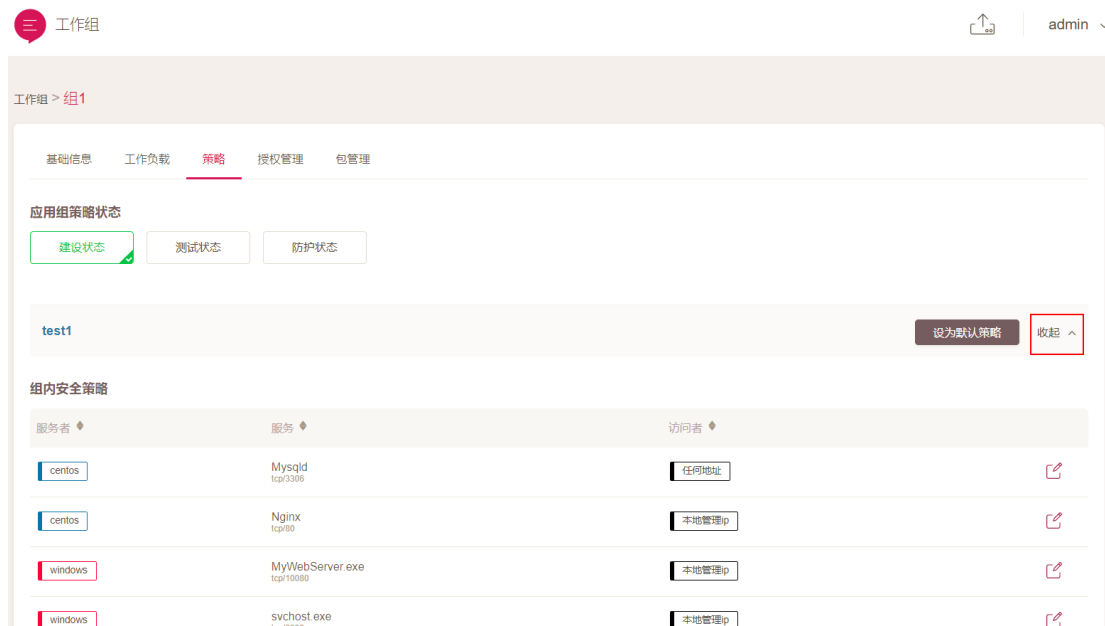
工作组 > 组1

基础信息 工作负载 策略 授权管理 包管理

应用组策略状态

建设状态 测试状态 防护状态

test1 设为默认策略 展开



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。

授权管理

admin

授权管理 > Cx5WJTSjXQ82pGKMiggAajEBGe2pFH9HMs4R9bMZ5Z9SGBzgausAmoNUwehsZUv

概要信息

授权码	Cx5WJTSjXQ82pGKMiggAajEBGe2pFH9HMs4R9bMZ5Z9SGBzgausAmoNUwehsZUv
创建人	admin
状态	
创建时间	2017-10-19 06:53:21

标签 允许自定义 数据库 测试环境 北京IDC

策略状态 不允许自定义

接入限制 无限制

有效期 永久

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。

工作组

admin

工作组 > 组1

基础信息 工作负载 策略 授权管理 **包管理**

包名称	最新版本	可升级	可安装
nodeclient	1.0.3	3	
collectclient	1.0.3	3	
fwclient	1.0.4	3	

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。

工作组 > 组1

基础信息 工作负载 策略 **授权管理** 包管理

包名称	最新版本	可升级	可安装
nodeclient	1.0.3	3	
collectclient	1.0.3	3	
fwclient	1.0.4	3	

升级 共 3 个工作负载 可升级 nodeclient 1.0.3 版本

<input type="checkbox"/>	主机名	IP	角色	当前版本	状态 ▾
<input type="checkbox"/>	ubuntu	192.168.247.165	ubuntu	1.0.2	初始态
<input type="checkbox"/>	ubuntu	192.168.247.157	ubuntu	1.0.2	初始态
<input type="checkbox"/>	ubuntu14	192.168.247.168	ubuntu	1.0.2	初始态

第1-3条 共3条 1 10条/页

3.2.5 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。

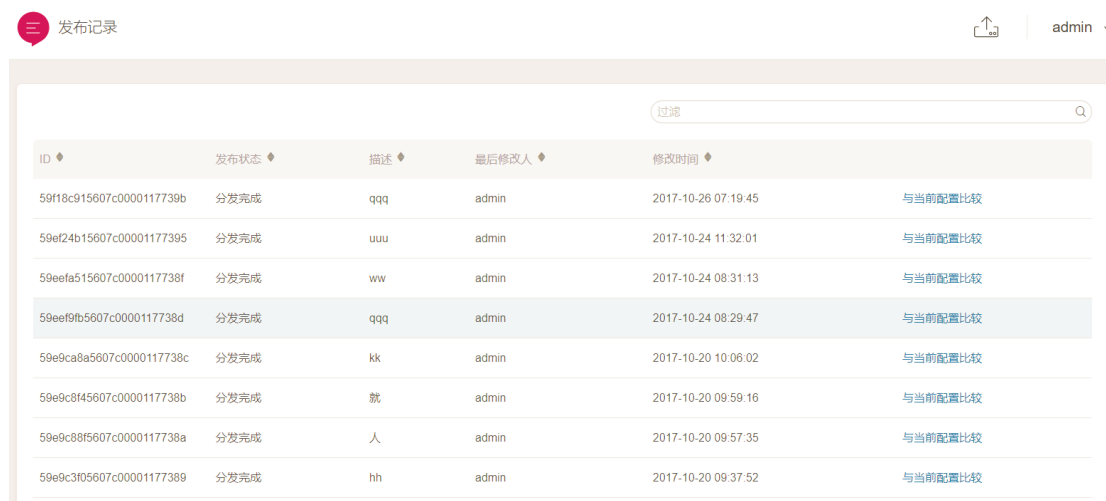


全部还原

2. 点击 [全部还原](#) 按钮，可将本次还未发布的操作进行还原。

3.2.6 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。



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

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

3.3 告警与事件

1. 点击菜单栏最下方告警与事件-操作日志，可进入操作日志界面。



操作日志会记录用户的操作，例如工作组的创建、策略的生成等等

操作日志

操作: [全部] 时间范围: 2018-06-12 15:54 ~ 2018-06-19 15:54 查询

导出

ID	操作时间	账户	动作	对象	条目	更改内容	执行状态
5b28b3d18bf54779dd30a0fa	2018-6-19 15:42:09	admin	修改	工作负载		工作组[idotoors]	成功
5b28b3a18bf54779dd3098b8	2018-6-19 15:41:21	admin	修改	工作负载		工作组[\$DEFAULTS]	成功
5b28b3888bf54779dd30961f	2018-6-19 15:40:56	admin	修改	服务对象	名字[Op@nvpn]	服务配置[tcp/11941,udp/11940,tcp/11941]	成功

2. 系统日志界面会记录系统的运行信息，包括 debug 信息、info 信息、告警信息等。