版 本 号：V1.0

文档标识：YY-GYY-AQFW-GGSM

安全服务V1. 0.0

需求规格说明书

产品部

2016年5月

**文档修改页**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 序号 | 版本号 | 修改内容 | 修改人 | 修改日期 |
|  | V0.1 | 建立文档 | 罗蕾 | 2016.5.24 |
|  | V0.2 | 防火墙规则增加调整优先级功能 | 罗蕾 | 2016.6.1 |
|  | V0.3 | 内部评审，修改防火墙规则列展示。 | 罗蕾 | 2016.6.8 |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

**目录**

[1 文档概述 5](#_Toc454530484)

[1.1 概述 5](#_Toc454530485)

[1.2 背景及目的 5](#_Toc454530486)

[1.3 功能范围 5](#_Toc454530487)

[2 功能列表 5](#_Toc454530488)

[3 管理控制台ECSC 6](#_Toc454530489)

[3.1 防火墙 6](#_Toc454530490)

[3.1.1. 查看防火墙 6](#_Toc454530491)

[3.1.2. 防火墙详情 8](#_Toc454530492)

[3.1.3. 创建防火墙 10](#_Toc454530493)

[3.1.4. 更新防火墙 12](#_Toc454530494)

[3.1.5. 标签 15](#_Toc454530495)

[3.1.6. 删除防火墙 16](#_Toc454530496)

[3.2 安全组 16](#_Toc454530497)

[3.2.1. 查看安全组 16](#_Toc454530498)

[3.2.2. 安全组详情 18](#_Toc454530499)

[3.2.3. 创建安全组 21](#_Toc454530500)

[3.2.4. 更新安全组 22](#_Toc454530501)

[3.2.5. 标签 27](#_Toc454530502)

[3.2.6. 删除安全组 28](#_Toc454530503)

[4 运维中心（ECMC） 28](#_Toc454530504)

[4.1. 防火墙 28](#_Toc454530505)

[4.1.1. 查看防火墙 28](#_Toc454530506)

[4.1.2. 防火墙详情 29](#_Toc454530507)

[4.1.3. 创建防火墙 29](#_Toc454530508)

[4.1.4. 更新防火墙 30](#_Toc454530509)

[4.1.5. 删除防火墙 31](#_Toc454530510)

[4.2. 安全组 31](#_Toc454530511)

[4.2.1. 查看安全组 31](#_Toc454530512)

[4.2.2. 安全组详情 31](#_Toc454530513)

[4.2.3. 创建安全组 32](#_Toc454530514)

[4.2.4. 更新安全组 32](#_Toc454530515)

[4.2.5. 删除安全组 32](#_Toc454530516)

[5 权限和日志 33](#_Toc454530517)

[5.1 ECSC 33](#_Toc454530518)

[5.1.1 权限 33](#_Toc454530519)

[5.1.2 日志 33](#_Toc454530520)

[5.2 ECMC 34](#_Toc454530521)

[5.2.1 权限 34](#_Toc454530522)

[5.2.2 日志 35](#_Toc454530523)

# 文档概述

## 概述

此文档描述了易云公有云安全服务V1.0.0版的完整需求，包括安全组、防火墙的功能、操作流程和原型界面。

## 背景及目的

易云公有云的安全模块提供了2级防火墙服务，主机级别的为安全组服务，路由级别为防火墙服务。安全组在主机的虚拟网卡上过滤流量包，防火墙则在路由器上进行流量过滤。目前易云公有云的防火墙和安全组在数据展现和操作逻辑仍然沿用OpenStack原生态模式，不方便用户的操作，故调研竞品厂商的数据展现及处理模式，结合我们公有云平台的现状，编写了安全服务v1.0.0的需求文档，优化安全模块的数据展现和操作流程。

## 功能范围

易云安全服务v1.0.0版本，其目标为：（1）优化防火墙和安全组的操作流程和数据展现；（2）提供面向用户的前台功能；（3）提供面向运维人员的后台管理功能；（4）支持上述业务必须的功能。

# 功能列表

表一 安全服务V1.0.0 功能列表

| **序号** | **功能模块** | **功能** | **描述** | **优先级** | **备注** |
| --- | --- | --- | --- | --- | --- |
| 1 | 防火墙 | 查看 | 查看防火墙列表和详情 | P1 | ECSC和ECMC中一致 |
| 2 | 创建 | 创建防火墙，同时创建规则 | P1 |
| 3 | 编辑 | 修改防火墙名称和描述 | P3 |
| 4 | 添加规则 | 添加防火墙规则 | P1 |
| 5 | 启用/禁用规则 | 可以开启和禁用防火墙中某一规则 | P2 |
| 6 | 调整优先级 | 调整某一规则在防火墙中的优先级。 | P2 |
| 7 | 删除规则 | 删除防火墙中的规则 | P1 |
| 8 | 删除 | 删除防火墙 | P1 |
| 9 | 标签 | 防火墙设置标签 | P2 | **仅ECSC中** |
| 10 | 安全组 | 查看 | 查看安全组列表及详情 | P1 | ECSC和ECMC中一致 |
| 11 | 创建 | 创建安全组 | P1 |
| 12 | 编辑 | 修改安全组名称和描述，默认安全组规则不可改 | P3 |
| 13 | 添加规则 | 添加安全组规则 | P1 |
| 14 | 删除规则 | 删除安全组规则 | P1 |
| 15 | 添加云主机 | 云主机加入安全组 | P2 |
| 16 | 移除云主机 | 云主机移除安全组 | P2 |
| 17 | 删除 | 删除安全组，默认安全组不可删除 | P1 |
| 18 | 标签 | 安全组设置标签 | P2 | **仅ECSC中** |

# 管理控制台ECSC

## 防火墙

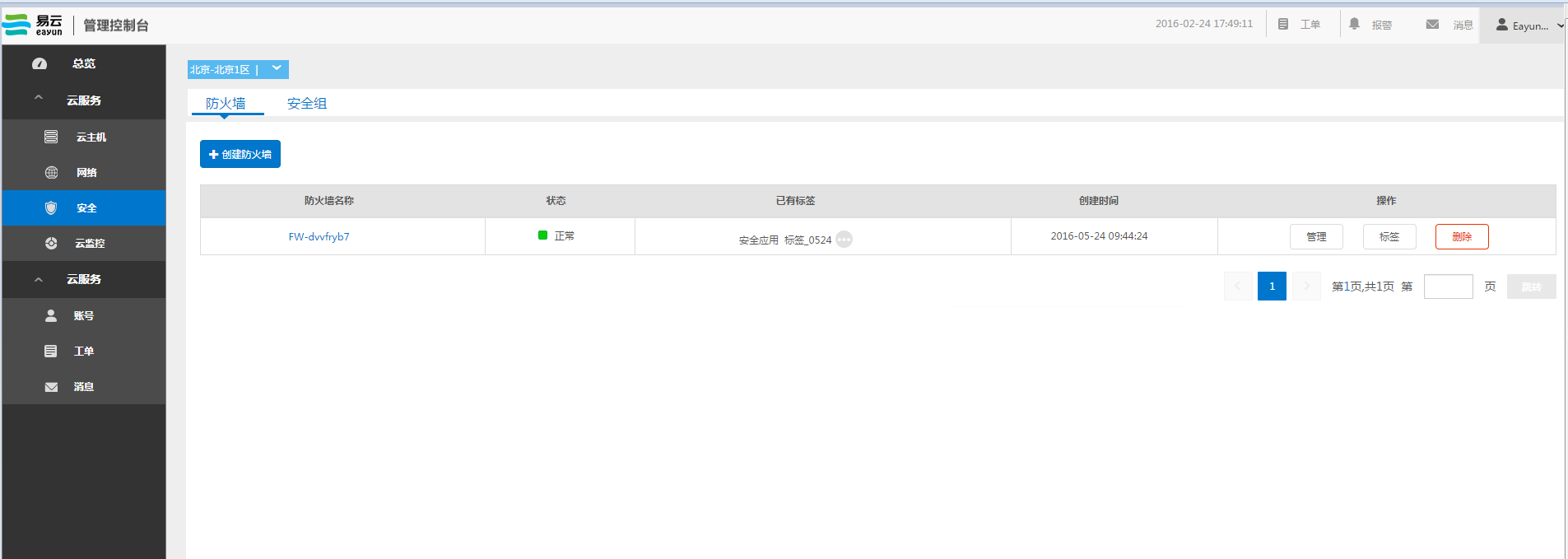
### 查看防火墙

#### 功能描述

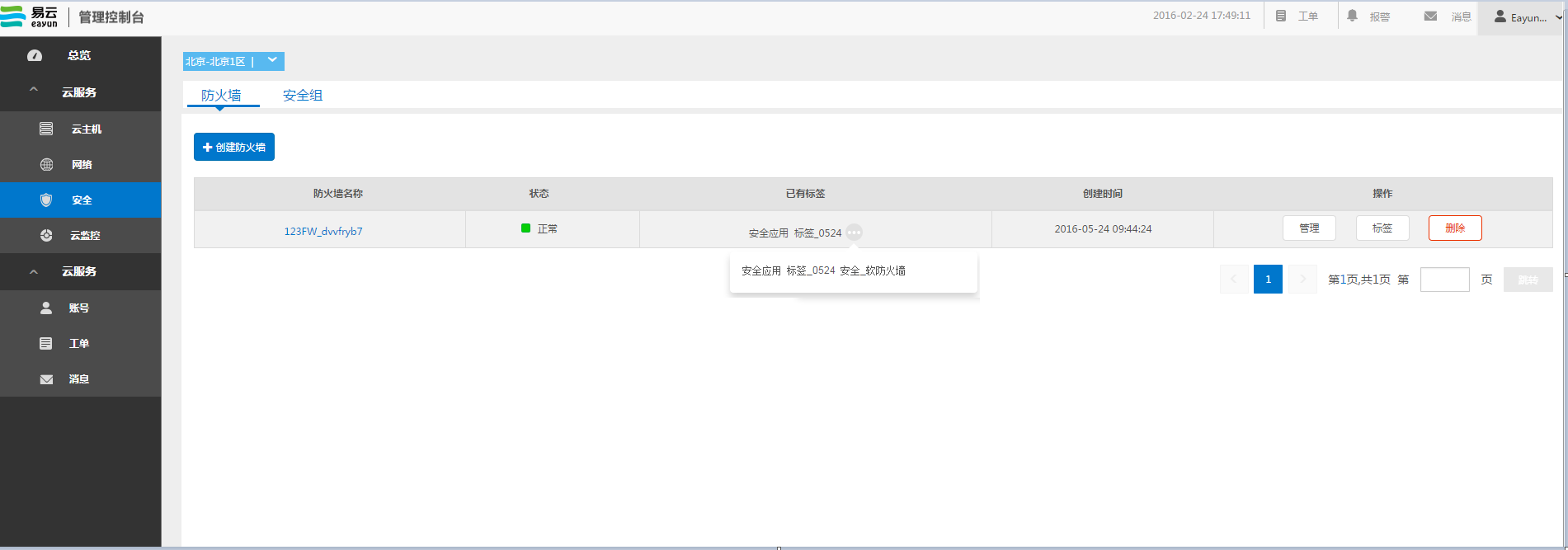
以列表的形式展示当前数据中心下的防火墙，提供创建、管理、标签及删除防火墙的入口。

#### 设计图

设计风格沿用ECSCv1.0.0，原型示意图如下：



图一 防火墙列表页面



图二 已有标签列展示

#### 规则说明

1. 列表展示数据项如下：

表二 防火墙列表字段说明

| **序号** | **展示数据项** | **说明** | **备注** |
| --- | --- | --- | --- |
| 1. | 防火墙名称 | 防火墙的名称 | 名称**蓝色标识**，点击可进入详情页 |
| 2. | 状态 | 标识防火墙的状态 | 状态展示中文名 |
| 3. | 已有标签 | 展示防火墙已设置的标签 | 同ECSCv1.0 |
| 4. | 创建时间 | 该防火墙的创建时间 | 新增项 |
| 5. | 操作 | 提供“管理”、“标签”和“删除”操作 |  |

1. 防火墙状态

表三 防火墙状态说明

| **序号** | **状态中文名** | **对应状态英文名** | **备注** |
| --- | --- | --- | --- |
| 1. | 创建中 | PENDING\_CREATE |  |
| 2. | 正常 | ACTIVE |  |
| 3. | 故障 | ERROR |  |
| 4. | 更新中 | PENDING\_UPDATE |  |
| 5. | 删除中 | PENDING\_DELETE |  |

1. 标签栏展示当前防火墙已设置的标签，若超过两个标签则带控件的…展示，放置在控件上展示所有已标注的所有标签。见“图二 已有标签列展示”
2. 点击防火墙名称或“管理”按钮，进入防火墙详情页面。

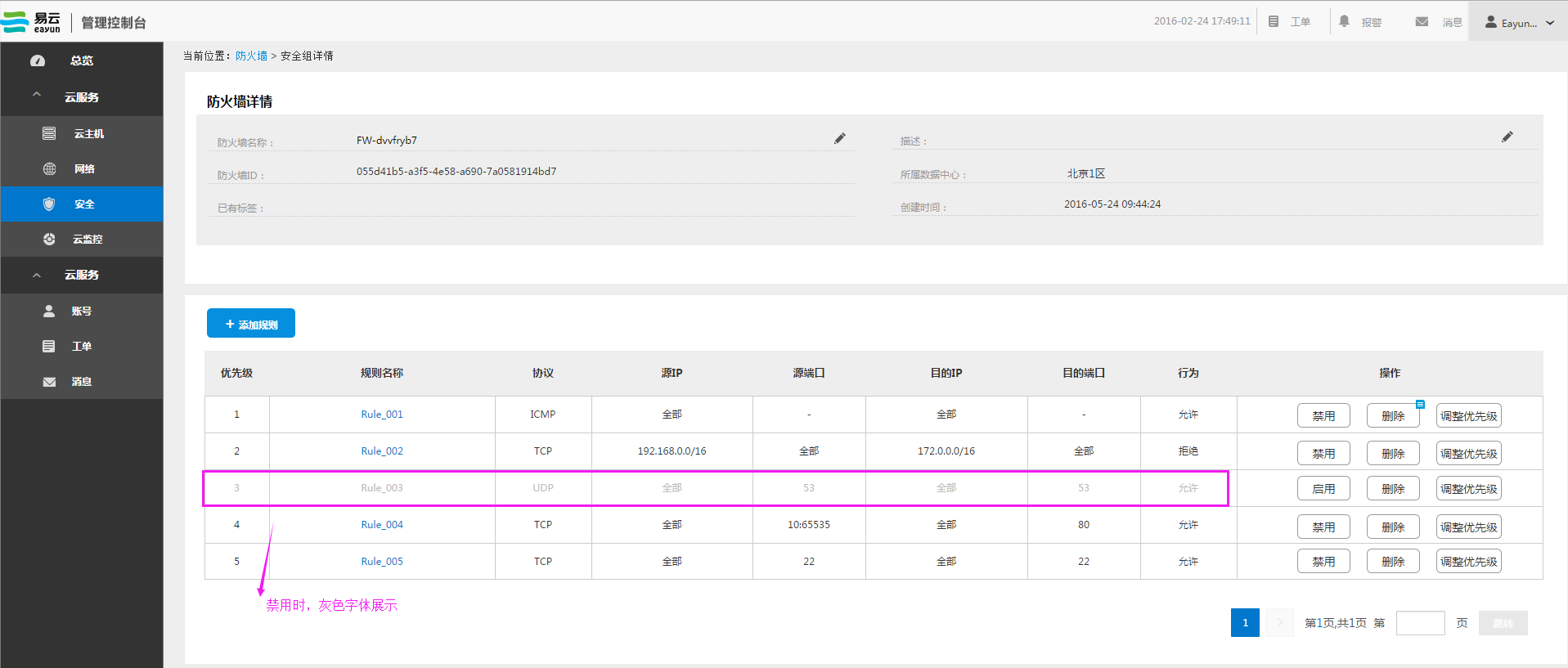
### 防火墙详情

#### 功能描述

提供防火墙详情展示、添加、删除、禁用/开启和查看规则的入口。

#### 设计图

设计风格沿用ECSCv1.0.0的整体风格，详情展示同安全组，原型示意如下：



图三 防火墙详情页

点击规则名称，可查看规则详情。



图四 防火墙规则详情

#### 规则说明

1. 基本信息：展示的参数项为防火墙名称、描述、防火墙ID、所属数据中心、已有标签、所属项目和**创建时间。**防火墙名称和描述可编辑修改，参数栏右侧可点击图标“”，可进行修改。
2. 操作按钮“添加规则”放置在防火墙规则列表上；
3. 列表中展示防火墙中已添加的规则，规则列表展示的字段如下：
4. **优先级：**标识当前规则在防火墙中的优先级，优先级按照由高到低排列，数字越小优先级越高；
5. **规则名称：**蓝色字体展示，点击后可查看规则详情，见“图四 防火墙规则详情”；
6. **协议：**当前规则的协议；
7. **源IP：**源IP地址或者IP地址段，例如：192.168.100.3或192.168.0.0/24；若是全部IP地址，则直接显示 “全部”；
8. **源端口**：源端口或者端口范围，例如：22 或22:100，若是全部端口则显示“全部”，ICMP协议端口参数不适用，该项数据展示为“-”；
9. **目的IP：**显示同源IP；
10. **目的端口：**显示同源端口；
11. **行为：**显示内容为“允许”或者“拒绝”；
12. **操作：**支持启用/禁用、删除和调整优先级操作，启用和禁用作为互斥按钮展示。
13. 防火墙规则，每一页最多展示10条记录，超过10条则分页展示。
14. 点击防火墙规则名称，进入规则详情页面，详情页展示的参数项为：**所属数据中心**、优先级、规则名称、协议、源IP、源端口、目的IP、目的端口、行为、**规则状态**和**创建时间**。

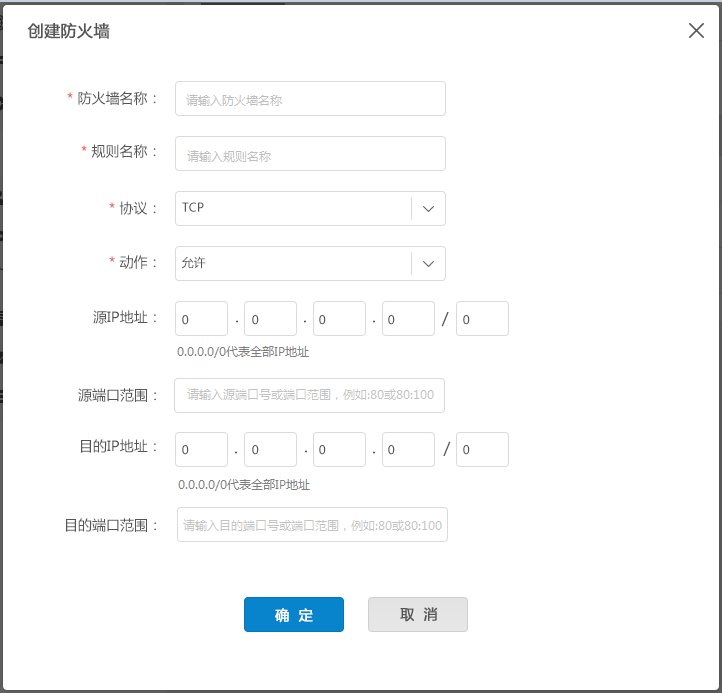
### 创建防火墙

#### 功能描述

简化了创建防火墙的流程，用户不需要先建防火墙规则和防火墙策略，创建防火墙时，同时设置防火墙规则。

#### 设计图

创建防火墙页面展如下：



图五 创建防火墙\_协议为TCP/UDP



图六 创建防火墙\_协议为ICMP/所有

#### 规则说明

1. 数据项说明

表四 创建防火墙页面参数说明

| **序号** | **参数项** | **必填项** | **说明** | **备注** |
| --- | --- | --- | --- | --- |
| 1. | 所属项目 | 是 |  | **去掉此项** |
| 2. | 防火墙名称 | 是 | 同ECSCv1.0 |  |
| 3. | 规则名称 | 是 | 同ECSCv1.0防火墙规则 |  |
| 4. | 协议 | 是 | 同ECSCv1.0 防火墙规则 | 协议“任何”修改为“所有” |
| 5. | 动作 | 是 | 同ECSCv1.0 防火墙规则 |  |
| 6. | 源IP地址 | 否 | 同ECSCv1.0 防火墙规则 | 样式见设计图 |
| 7. | 源端口范围 | 否 | 同ECSCv1.0 防火墙规则 |  |
| 8. | 目的IP地址 | 否 | 同ECSCv1.0 防火墙规则 | 样式见设计图 |
| 9. | 目的端口范围 | 否 | 同ECSCv1.0 防火墙规则 |  |

1. 参数项限定说明
2. **所属项目**：**去掉**所属项目，创建的防火墙默认当前客户在导航栏选中的数据中心下。
3. **防火墙名称**：必填项，同一项目下仅可创建一个防火墙。长度限定为20位，支持数字、中英文、下划线和空格，不能以下划线开头或结尾；
4. **规则名称**：必填项，同一项目下名称必须唯一，对于客户而言同一数据中心下唯一；长度限定为20位，支持数字、中英文、下划线和空格，不能以下划线开头或结尾；
5. **协议**：必选项，默认选择“TCP”，下拉列表展示值为“TCP”、“UDP”、“ICMP”和“所有”；
6. **动作**：必选项，默认选择“允许”，下拉列表值为“允许”和“拒绝”；
7. **源/目的IP地址：**地址格式为 X.X.X.X/Y,默认值为0.0.0.0/0,表示所有IP地址；X的取值范围为：0-255，Y的取值范围为0-32；当光标放入前四位的输入框时，默认提示：“请输入0到255的整数” ，当光标放入Y位置的输入框时，默认提示：“请输入0到32的整数”；
8. **源/目的端口范围：**

1)当协议选择TCP或者UDP时，源/目的端口范围才可用，选择ICMP和所有时，该项参数隐藏；

2)输入框中默认提示信息为“请输入源端口号或端口范围，例如:80或80:100”或“请输入目的端口号或端口范围，例如:80或80:100”；

3)此项输入为端口号或者端口范围，合法格式为A或A:B，其中A和B的取值范围为1-65535；

4)输入非法时提示：“端口格式为A或A:B，其中A和B范围为1-65535”。

1. 其他说明

ECSCv1.0中创建防火墙时，需要先创建规则，再创建策略并绑定规则，最后才能创建防火墙，此版隐藏防火墙策略的相关信息，同时在防火墙的详情页中，管理防火墙规则。

创建防火墙时后台自动生成防火墙策略，同时将设置的规则自动绑定到自动生成的防火墙策略中，同时将该策略自动关联到防火墙上，在详情页中再添加规则时，则规则自动绑定到后台默认生成的策略上。

当协议类型选择ICMP时，端口值参数无效，故添加成功后，列表中源端口和目的端口值展示“-”（ ECSCv1.0中规则列表，ICMP协议显示为“全部”，需要调整为“-”，表示不适用）。

### 更新防火墙

#### 功能说明

更新防火墙包括，编辑防火墙名称和描述，给防火墙添加规则、删除规则、禁用/启用规则和移动规则。

#### 规则说明

##### 编辑防火墙

在防火墙详情页面，点击名称和描述栏右侧的图标“”，可进行修改名称和描述信息。

**名称：**修改规则同添加规则，长度限定为20位，支持数字、中英文、下划线和空格，不能以下划线开头或结尾。

**描述信息：**长度限定为200位，描述不为必填项，超过40位则采用带图标的“”展示。

##### 添加规则

添加规则页面同创建防火墙页面相比，**无**防火墙名称字段，各项参数限定同添加防火墙页面，最新创建的规则排在最前边，且优先级最高（优先级数字值越低，优先级越高）效果图如下：



图七 添加防火墙规则\_TCP/UDP



图八 添加防火墙规则\_ICMP/所有

##### 禁用/启用规则

（1）**禁用规则：**

当规则状态为“已启用”时，显示“禁用”按钮，点击禁用按钮后，给出二级确认提示，提示：“确定要禁用规则XXX”，XXX为规则名称，点击确定按钮后，页面中该条规则参数字体灰置（BDBDBD）展示，该规则变为“已禁用”状态，同时详情页中该规则状态也显示为“已禁用”。规则禁用后，该条规则不起作用。

（2）**启用规则**：

当规则为“已禁用”状态时，显示“启用”按钮，点击启用按钮后，给出二级确认提示，提示：“确定要启用规则XXX”，XXX为规则名称，点击确定按钮后，该规则变为“已启用”状态。规则重新启用后，能成功允许或拒绝满足该条规则的流量通过。

##### 删除规则

点击删除按钮后，给出确认提示“确定要删除规则XXX” ，XXX为规则名称，点击确定按钮后，执行删除规则操作。

注：此版无防火墙策略的概念，执行删除时，后台需要先将该规则与默认策略解绑，然后再执行删除操作。

##### 调整优先级

在操作列点击“调整优先级”按钮，进入调整优先级操作页面，原型示意图如下：



图九 调整优先级

调整优先级时，需要设置当前规则优先级低于或高于某条规则，则页面的参数项有：调整规则、插入（前于或后于）、规则名称。

1. 调整规则：显示欲调整优先级规则的名称，只读项显示当前
2. 插入：前于表示移动该规则位于选中规则的前边，后于表示移动规则位于选中规则的后边；
3. 规则名称：下拉列表中展示除去自身规则外其他所有已加入该防火墙的规则；
4. 保存成功后，列表中规则的优先级成功更新。

例如：当前防火墙规则的优先级顺序为：1-R1、2-R2、3-R5、4-R3，要调整R3的优先级，选定插入位置前于规则R5，点击确定按钮，保存成功后，其规则优先级顺序为：1-R1、2-R2、3-R3、4-R5。

注：底层无直接调整规则优先级的接口，在调整优先级时后台需要先自动移除该规则，然后插入到页面设置的位置。

### 标签

在防火墙列表中点击“标签”按钮，可以给防火墙设置标签，标签功能作为通用功能，处理逻辑同标签模块。

当标签超过三个时，防火墙列表和详情页的标签栏中采用带图标的“”展示，鼠标移动至图标时展示所有的标签信息。

### 删除防火墙

点击删除按钮后，给出确认提示“删除后网络下的流量将不受限制，确定要删除防火墙？” ，点击确定按钮后，执行删除操作，删除防火墙时会自动删除掉关联该防火墙的所有规则，同时后台也会删除默认生成的防火墙策略。

## 安全组

### 查看安全组

#### 功能描述

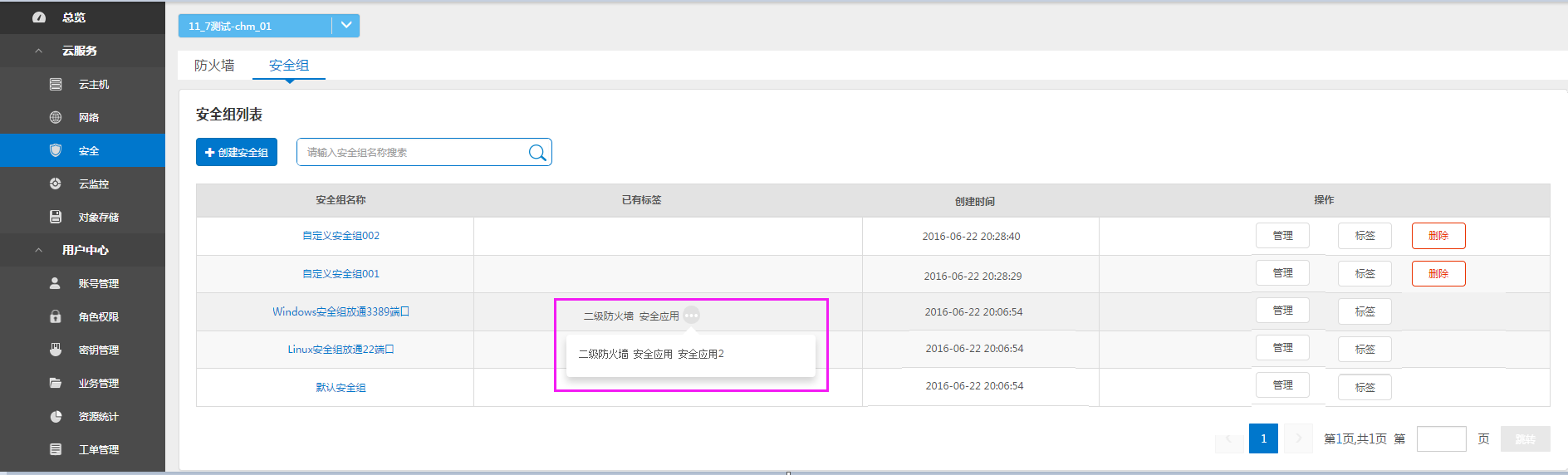
以列表的形式展示当前数据中心下所有的安全组，提供创建、查询、管理、标签及删除安全组的入口。

#### 设计图

安全组列表沿用ECSCv1.0.0的风格，展示数据项参照原型图，其原型示意图如下：



图十 安全组列表



图十一 已有标签列展示

#### 规则说明

1. 列表展示数据项如下：

表五 安全组列表字段说明

| **序号** | **展示数据项** | **说明** | **备注** |
| --- | --- | --- | --- |
| 1. | 安全组名称 | 安全组的名称 | 名称**蓝色标识**，点击可进入详情页 |
| 2. | 已有标签 | 展示安全组已设置的标签 |  |
| 3. | 创建时间 | 该安全组的创建时间，系统内置安全组创建时间读取创建项目的时间 | **新增数据项** |
| 4. | 操作 | 提供“管理”、“标签”和“删除”操作 |  |

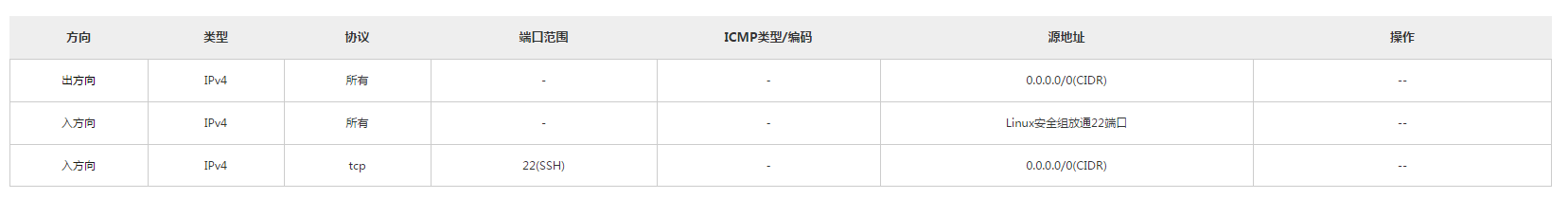
1. 创建项目时系统默认会生成3个安全组，名称分别为“默认安全组”、“Linux安全组放通22端口”和“Windows安全组放通3389端口”。

* 默认安全组：对应先前的defaut安全组，此版更名为“默认安全组”。
* Linux安全组放通22端口：创建项目时后台默认生成。其规则如下，

出方向：放通所有流量；

入方向：放通与当前安全组关联云主机的所有流量；

入方向：放通SSH连接所有IP地址的流量。



* Windows安全组放通3389端口：创建项目时后台默认生成。其规则如下，

出方向：放通所有流量；

入方向：放通与当前安全组关联云主机的所有流量；

入方向：放通SSH连接所有IP地址的流量。



1. 系统内置的3个安全组的创建时间读取该项目的创建时间；
2. 标签栏展示当前防火墙已设置的标签，若超过两个标签则带控件的“”展示，放置在控件上展示所有已标注的所有标签。见“图十 已有标签列展示”；
3. 点击安全组名称或“管理”按钮，进入安全组详情页面。

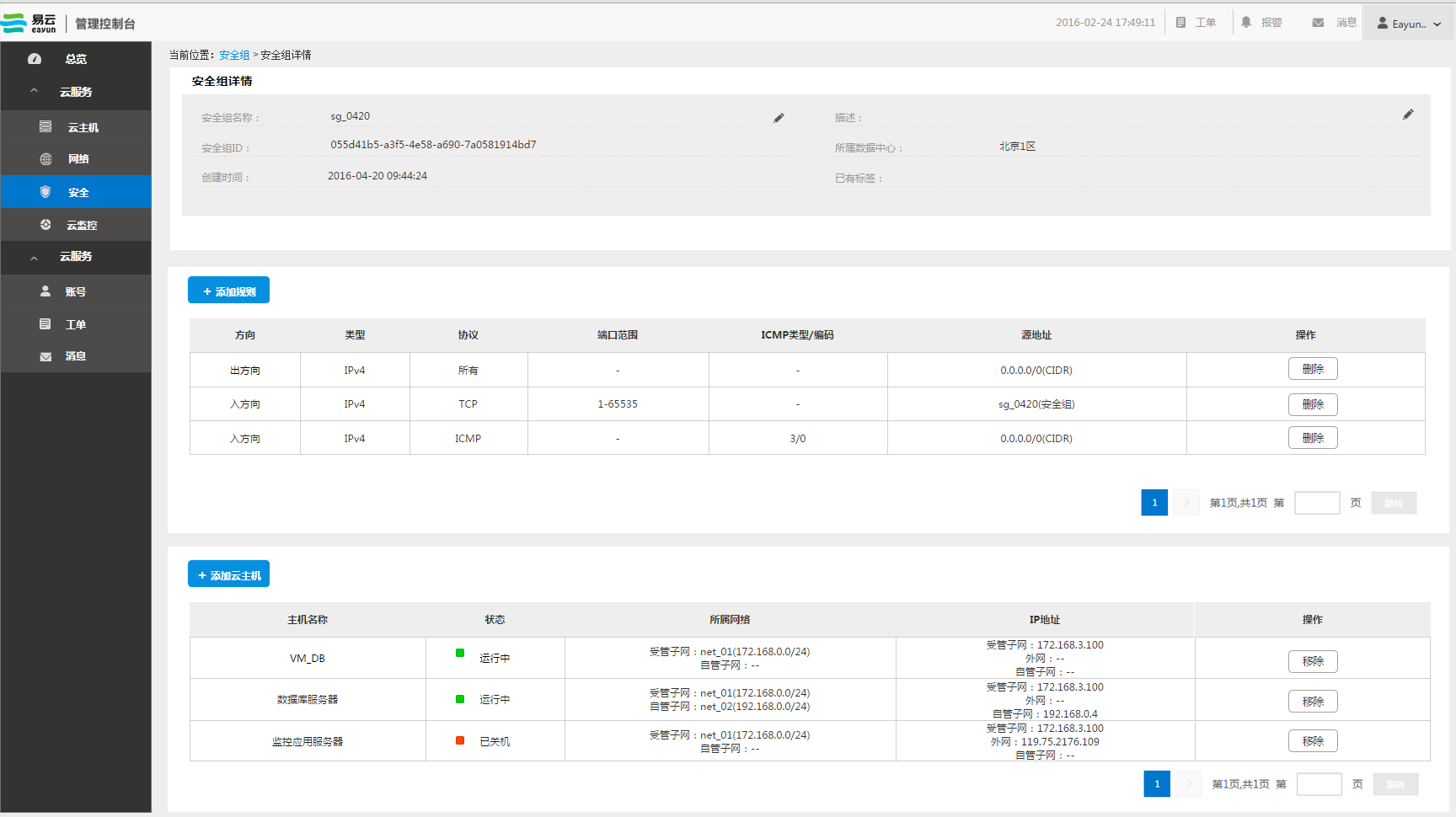
### 安全组详情

#### 功能描述

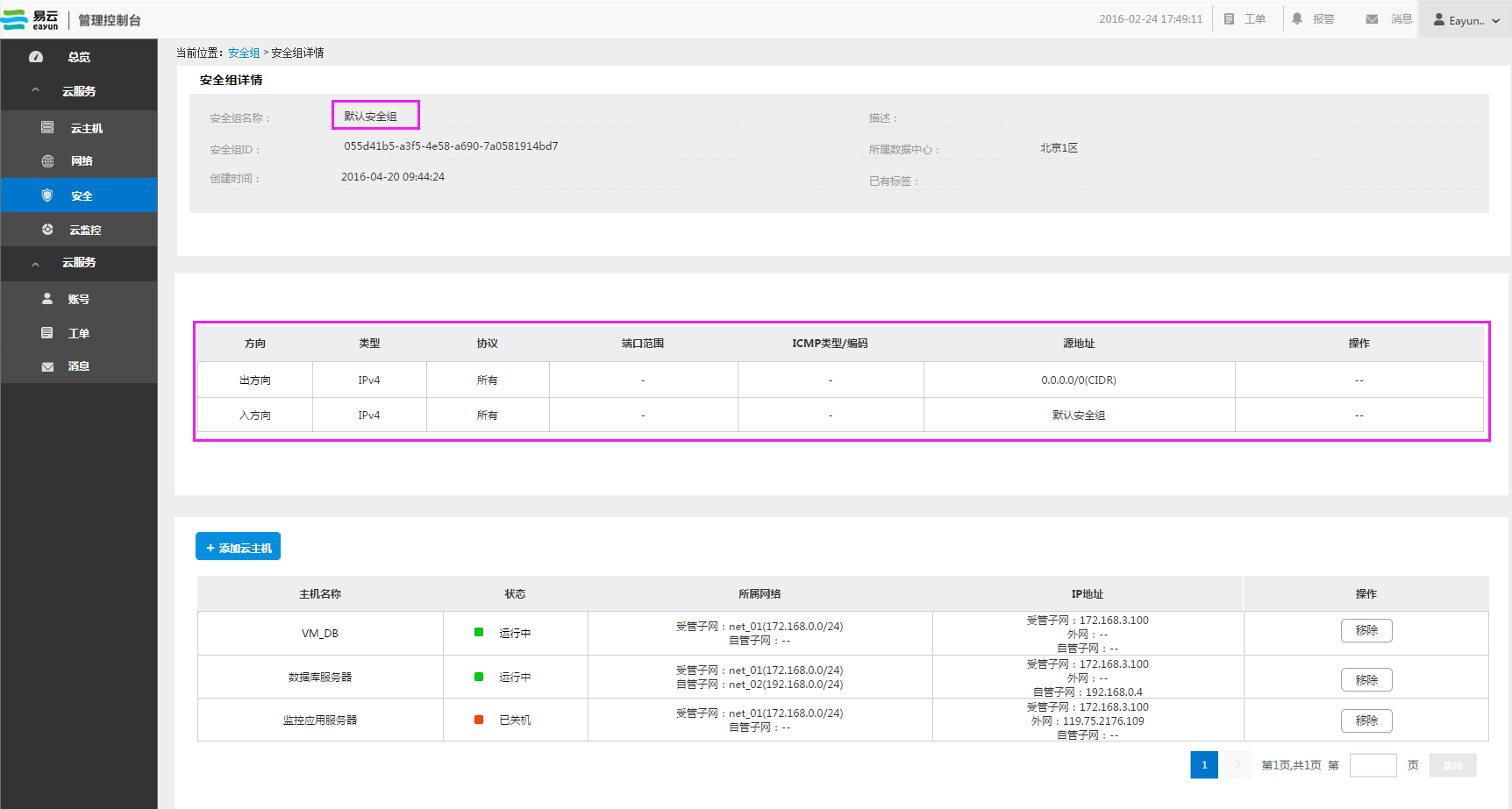
提供安全组详情展示、添加、删除和查看规则的入口。

#### 设计图

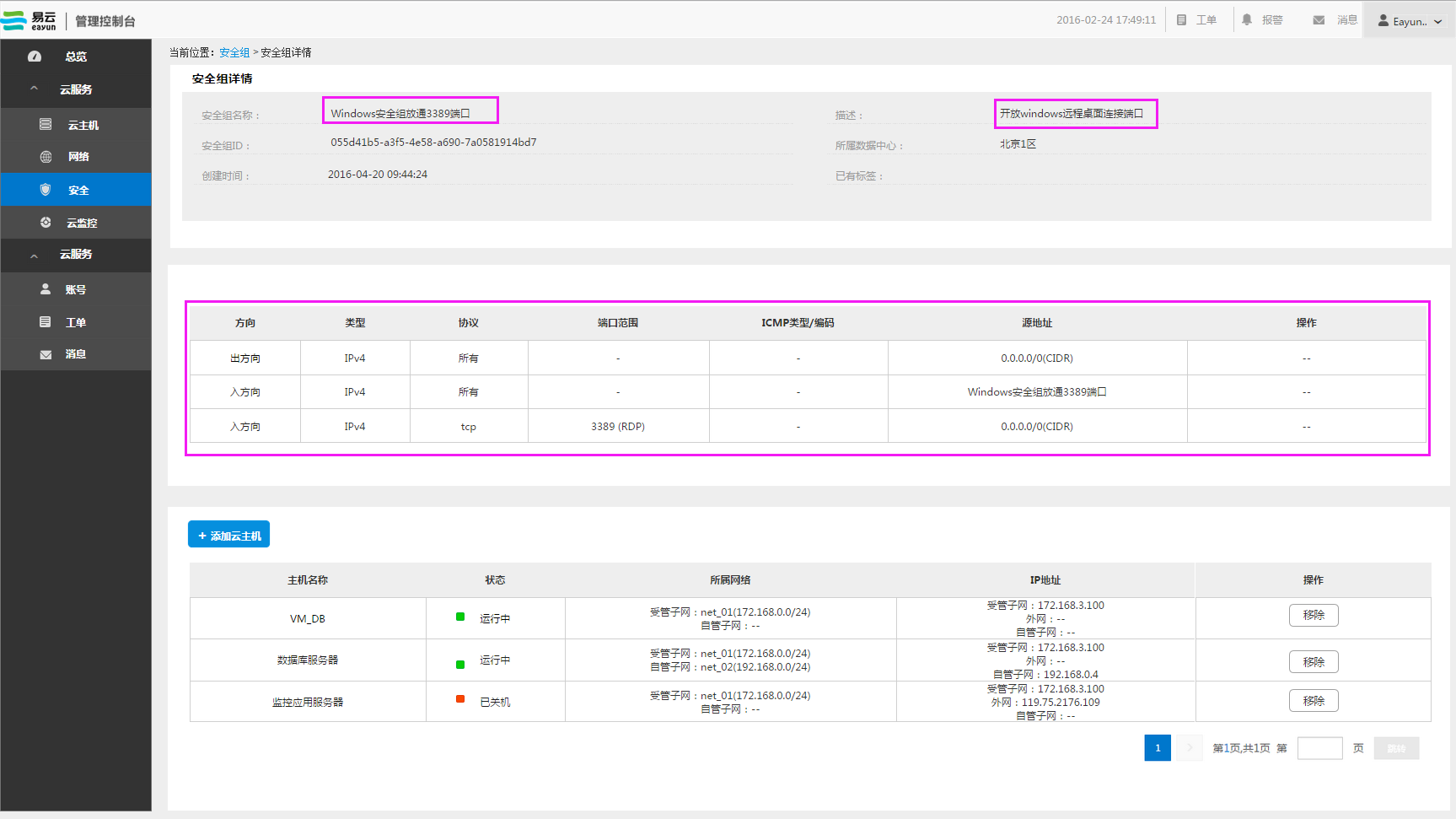
安全组详情设计风格沿用ECSCv1.0.0，其原型示意如下：



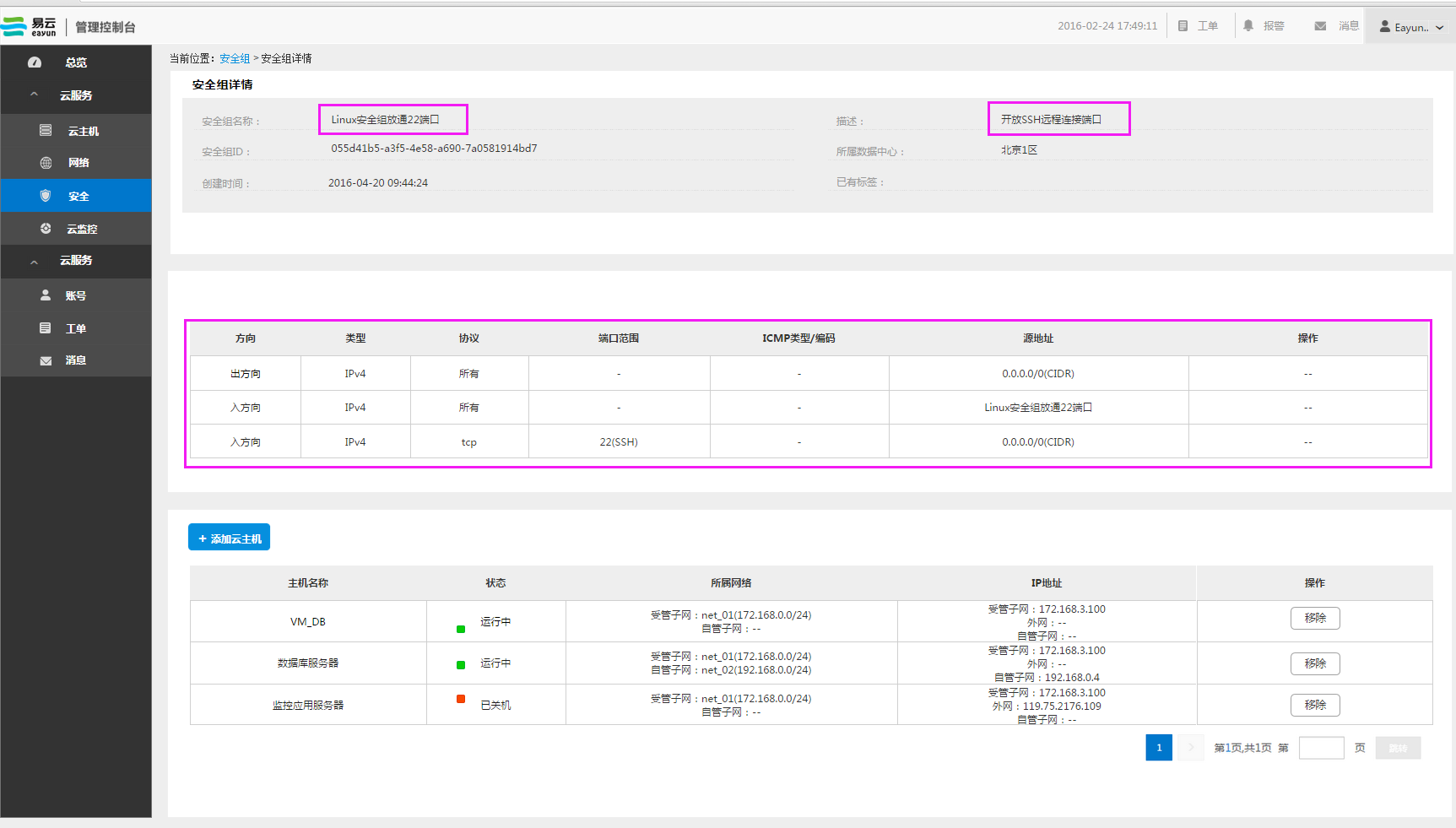
图十二 安全组详情页



图十三 安全组详情页\_默认安全组



图十四 安全组详情页\_Windows安全组放通3389端口



图十五 安全组详情页\_Linux安全组放通22端口

#### 规则说明

1. 基本信息：

展示的参数项为安全组名称、描述、安全组ID、所属数据中心、已有标签和创建时间，**去掉**所属项目。用户自己创建的安全组名称和描述可编辑修改，参数栏右侧可点击图标“”，可进行修改；系统默认的安全组，名称和描述都不可更改。

1. 规则列表：
2. 添加规则按钮移动至规则列表上，见“图十一 安全组详情页”；
3. “默认安全组”、“Linux安全组放通22端口”和“Windows安全组放通3389端口”详情页中**无**添加规则按钮，同时也**无**删除默认规则的按钮。
4. 安全组规则列表展示的数据项，说明如下：

表六 安全组规则列表参数说明

| **序号** | **展示数据项** | **说明** | **备注** |
| --- | --- | --- | --- |
| 1. | 方向 | 标识是“出方向”或“入方向”的流量 | 对应ECSCv1.0中的“出口”和“入口” |
| 2. | 类型 | 展示以太网类型 | 目前仅支持IPv4 |
| 3. | 协议 | 展示该条规则的协议 | 同ECSCv1.0 |
| 4. | 端口范围 | 仅展示端口范围值 | 协议为ICMP时，此列不适用，展示为“-” |
| 5. | ICMP类型/编码 | 协议为ICMP时，此列有数据。其他则展示‘-’ | **新增数据列** |
| 6. | 源地址 | 标识作用端，显示安全组或者CIDR地址 | 同ECSCv1.0中的远程 |
| 7. | 操作 | 提供“删除”操作按钮 | 同ECSCv1.0 |

1. 安全组规则每页展示5条，超过5条则分页展示。
2. 云主机列表（**新增功能**）
3. “添加云主机”按钮放置在云主机列表上，见“图十一 安全组详情页”；
4. 云主机列表展示的数据项，说明如下：

表七 云主机列表字段说明

| **序号** | **展示数据项** | **说明** | **备注** |
| --- | --- | --- | --- |
| 1. | 主机名称 | 已加入该安全组的主机名称 |  |
| 2. | 状态 | 展示该云主机的状态 |  |
| 3. | 所属网络 | 主机所在的子网，显示格式为：  受管子网：net\_01(172.168.0.0/24)  自管子网：-- |  |
| 4. | IP地址 | 显示该主机的IP地址，无外网时，显示“--” |  |
| 5. | 操作 | 支持“移除”操作按钮 | 将云主机从安全组中移除。 |

1. 安全组规则每页展示5条，超过5条则分页展示。

### 创建安全组

创建安全组页面沿用ECSCv1.0，如下：



图十六 创建安全组

安全组的名称：由同一数据中心下唯一，**修改为**同一项目下唯一。同时**去掉**所属项目，创建的安全组默认当前客户在导航栏选中的数据中心下，其他处理逻辑不变，沿用ECSCv1.0。

### 更新安全组

#### 功能说明

更新安全组包括，编辑安全组名称和描述，给安全组添加/删除规则、安全组中添加/删除主机。

#### 规则描述

##### 编辑安全组

同ECSCv1.0相比，安全组“编辑”功能做如下调整：

1. 安全组列表中去掉编辑按钮，编辑操作仅可在详情页中操作；
2. 对于用户创建的安全组，在安全组详情页面，点击名称和描述栏右侧的图标“ ”，可进行修改名称和描述信息。

名称：修改规则同添加规则，长度限定为20位，支持数字、中英文、下划线和空格，不能以下划线开头或结尾。

描述信息：长度限定为200位，描述不为必填项。

##### 添加规则

在安全组的详情页中点击“添加规则”按钮，进入添加规则页面，设计图如下：



图十七 添加规则\_TCP和UDP页面



图十八 添加规则ICMP页面

1. 数据项说明
2. 添加规则页面参数说明

表八 添加安全组规则页面参数说明

| **序号** | **参数项** | **说明** | **备注** |
| --- | --- | --- | --- |
| 1. | 协议 | 下拉参数项有TCP、UDP和ICMP | 默认选中TCP |
| 2. | 方向 | 指定当前规则限定虚拟网卡“入方向”或“出方向”的流量 | 分别对应ECSCv1.0中的“入口”和“出口” |
| 3. | 起始端口 | 输入范围限定为1-65535的整数 | 同ECSCv1.0 |
| 4. | 结束端口 | 输入范围限定为1-65535的整数，必须≥起始端口 | 同ECSCv1.0 |
| 5. | ICMP类型 | 协议类型为“ICMP”时展示，可选类型见“表九 ICMP类型/编码下拉参数值说明” | 修改原来的输入框为下拉选择框。 |
| 6. | ICMP编码 | 协议类型为“ICMP”时展示，可选编码见 “表九 ICMP类型/编码下拉参数值说明” |
| 7. | 源地址 | 可选择“IP地址”或“安全组” | 同ECSCv1.0 远程 |
| 8. | IP地址 | 源地址选择“IP地址”时可设置，选择安全组不展示此项参数。 | **输入框已优化，见设计图** |
| 9. | 安全组 | 源地址选择“安全组”时可选择，选择IP地址时不展示此项参数。 | 同ECSCv1.0 |
| 10. | 常用规则 | 比较常用的规则，作为快捷方式列出。选择常用规则时，页面展示信息见表 | **见设计图** |

1. ICMP类型/编码下拉表中参数值

表九 ICMP类型/编码下拉参数值说明

| **序号** | **ICMP类型** | **ICMP编码** | **ICMP类型/编码列展示** |
| --- | --- | --- | --- |
| 1 | 所有 | 所有 | 所有 |
| 2 | 0-回应应答 | 0-Echo响应 | 0/0 |
| 3 | 3-目的地不可达 | 0-目标网络不可达 | 3/0 |
| 4 | 1-目标主机不可达 | 3/1 |
| 5 | 2-目标协议不可达 | 3/2 |
| 6 | 3-目标端口不可达 | 3/3 |
| 7 | 4-要求分段并设置DF flag标志 | 3/4 |
| 8 | 5-源路由失败 | 3/5 |
| 9 | 6-未知的目标网络 | 3/6 |
| 10 | 7-未知的目标主机 | 3/7 |
| 11 | 8-源主机隔离 | 3/8 |
| 12 | 9-禁止访问的网络 | 3/9 |
| 13 | 10-禁止访问的主机 | 3/10 |
| 14 | 11-由于服务类型为TOS，网络不可达 | 3/11 |
| 15 | 12-由于服务类型为TOS，主机不可达 | 3/12 |
| 16 | 13-网络流量被禁止 | 3/13 |
| 17 | 14-主机越权 | 3/14 |
| 18 | 15-优先中止生效 | 3/15 |
| 19 | 4-源端被关闭 | 0-源端被关闭（基本流量控制） | 4/0 |
| 20 | 5-重定向 | 0-重定向网络 | 5/0 |
| 21 | 1-重定向主机 | 5/1 |
| 22 | 2-对服务类型和网络重定向 | 5/2 |
| 23 | 3-对服务类型和主机重定向 | 5/3 |
| 24 | 8-回应请求 | 0-Echo请求 | 8/0 |
| 25 | 9-路由建议 | 0-路由建议 | 9/0 |
| 26 | 10-路由器请求 | 0-路由发现/选择/请求 | 10/0 |
| 27 | 11-超时 | 0-TTL在传输中过期 | 11/0 |
| 28 | 1-在数据包组装期间生存时间为0 | 11/1 |
| 29 | 12-参数错误 | 0-错误的IP首部 | 12/0 |
| 30 | 1-缺少必须选项 | 12/1 |
| 31 | 2-不支持的长度 | 12/2 |
| 32 | 13-时间戳请求 | 0-时间戳请求 | 13/0 |
| 33 | 14-时间戳应答 | 0-时间戳应答 | 14/0 |
| 34 | 15-信息请求 | 0-信息请求 | 15/0 |
| 35 | 16-信息应答 | 0-信息应答 | 16/0 |
| 36 | 17-地址掩码请求 | 0-地址掩码请求 | 17/0 |
| 37 | 18-地址掩码应答 | 0-地址掩码应答 | 18/0 |

1. ICMP类型下拉框中展示的值，见上表第2列“ICMP类型”；
2. 当选择ICMP类型时，ICMP编码下拉列表框中展示的值见上表第3列“ICMP编码”，切换不同的ICMP类型，ICMP编码下拉列表中展示不同的值；
3. 设置ICMP类型和编码，保存成功后，安全组规则列表“ICMP类型/编码”列，展示值对应上表第4列。
4. 常用规则说明

页面把常用规则通过快捷键的方式列出，选中后自动填充参数，常用规则参数说明如下表：

表十 常用规则对应字段展示表

| **序号** | **协议** | **常用规则** | **起始端口** | **终止端口** | **ICMP类型** | **ICMP编码** | **备注** |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 1 | TCP | ALL TCP | 1 | 65535 | - | - | 列表中端口范围展示“1-65535”； |
| 2 | UDP | ALL UDP | 1 | 65535 | - | - | 列表中端口范围展示“1-65535” |
| 3 | ICMP | ALL ICMP | - | - | 所有 | 所有 | 列表中ICMP类型/编码列展示 “所有” |
| 4 | UDP | DNS | 53 | 53 | - | - | 列表中端口范围展示“53(DNS)” |
| 7 | TCP | HTTP | 80 | 80 | - | - | 列表中端口范围展示“80(HTTP)” |
| 8 | TCP | HTTPS | 443 | 443 | - | - | 列表中端口范围展示“443(HTTPS)” |
| 9 | TCP | IMAP | 143 | 143 | - | - | 列表中端口范围展示“143(IMAP)” |
| 10 | TCP | IMAPS | 993 | 993 | - | - | 列表中端口范围展示“993(IMAPS)” |
| 11 | TCP | LADP | 389 | 389 | - | - | 列表中端口范围展示“389(LADP)” |
| 12 | TCP | MS SQL | 1443 | 1443 | - | - | 列表中端口范围展示“1443(MS SQL)” |
| 13 | TCP | MySQL | 3306 | 3306 | - | - | 列表中端口范围展示“3306(MySQL)” |
| 14 | TCP | POP3 | 110 | 110 | - | - | 列表中端口范围展示“110(POP3)” |
| 15 | TCP | POP3S | 995 | 995 | - | - | 列表中端口范围展示“995(POP3S)” |
| 16 | TCP | RDP | 3389 | 3389 | - | - | 列表中端口范围展示“3389(RDP)” |
| 17 | TCP | SMTP | 25 | 25 | - | - | 列表中端口范围展示“25(SMTP)” |
| 18 | TCP | SMTPS | 465 | 465 | - | - | 列表中端口范围展示“465(SMTPS)” |
| 19 | TCP | SSH | 22 | 22 | - | - | 列表中端口范围展示“22(SSH)” |

1. 选中TCP和UDP协议的常用规则时，展示起始端口号和终止端口号（页面参数见“图十四 添加规则\_TCP和UDP页面”）；选中ICMP协议的常用规则时，展示ICMP类型和ICMP编码（页面参数见“图十五 添加规则ICMP页面”）。
2. 当选中常用规则时，“协议”、“起始和终止端口号”或“ICMP类型和编码”自动选中和填入数据，对应的数据见上表。

**例如：**当选中SSH时，协议字段选中TCP、起始端口号展示为22，终止端口号展示为22,添加成功后规则列表端口范围展示“22(SSH)”，ICMP类型/编码列展示“-”。

当选中ALL ICMP时，协议字段选中ICMP，ICMP类型选中所有，ICMP编码选中所有，添加成功后规则列表端口范围展示“-”，ICMP类型/编码列展示“所有”。

1. 若选择常用规则后， “协议”、“起始和终止端口号”或“ICMP类型和编码”字段后仍然可以修改，常用规则只作为快捷填充，填充后用户也可手动修改（选择常用规则后，用户仍然可修改协议规则，手动修改后界面不做手动填入的数据是否与常用规则匹配的校验），添加成功后其规则同手动修改设置的参数值一致。
2. TCP和UDP协议类的常用规则添加成功后，其规则列表中端口范围展示见备注列，ICMP类型/编码列展示 “-”；若是添加的ALL ICMP 协议，其ICMP类型/编码列展示 “所有”，端口范围展示“-”。

注：“-”表示不实用。

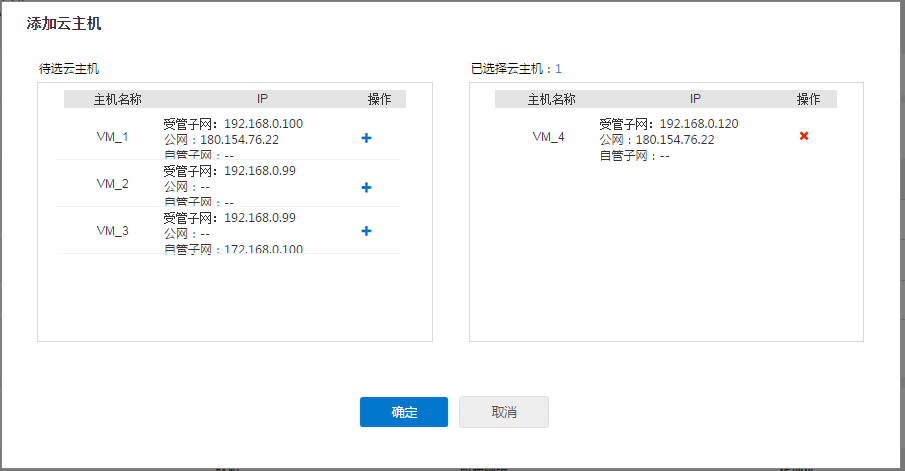
##### 删除规则

点击删除按钮后，给出确认提示“确定要删除规则“XXX”？” XXX格式为“‘方向’/‘协议’/‘端口范围’/‘ICMP类型编码’/‘源地址’”；点击确定按钮后，执行删除规则操作。

例如：确定要删除规则“‘出方向’/‘TCP’ /‘1-65535’/‘-’/‘SG\_001’”?确定要删除规则“‘入方向’/‘ICMP’/‘-’/‘3/5’/‘192.168.0.0’/‘16’” ？

##### 添加云主机至安全组

在安全组的详情页点击“添加云主机”，进入添加云主机页面，设计图如下：



图十九 添加云主机操作页面

1. 待选云主机列表中展示**当前项目下还未加入该安全组**的所有云主机（已欠费、已过期和已删除的云主机需要过滤掉）；点击“”后，成功移入右侧，在已选择云主机下点击“”后，该主机移入左侧；
2. 展示的主机参数为 主机名称、IP 和操作，数据展示见上图所示；
3. 未选择主机时，确定按钮置灰。

注：此处只能添加主机，不可移除已在安全组中的主机。移除主机的唯一入口进列表中的“删除”按钮。

##### 云主机移除安全组

在安全组的详情页的云主机列表下，提供“移除”按钮。点击移除按钮后，给出二级确认提示：“确定要将云主机XXX从安全组中移除？”XXX指代云主机的名称；点击确定按钮后云主机从安全组中成功移除，当前列表中不展示该云主机，同时云主机详情页不展示该安全组。

### 标签

在安全组列表中点击“标签”按钮，可以给安全组设置标签，标签功能作为通用功能，处理逻辑同标签模块。

当标签超过三个时，安全组列表和详情页的标签栏中采用带图标的“”展示，鼠标移动至图标时展示所有的标签信息。

### 删除安全组

ECSCv1.0中若安全组被云主机使用，则不允许删除。此版本**去掉**此限定条件，用户自己创建的安全组删除时无任何限定条件，点击删除按钮后，给出二级确认提示：“确定要删除安全组XXX” ，XXX为安全组名称，点击确定按钮后，执行删除规则操作。删除成功后，要清除安全组和云主机的关系表，同时在云主机的详情页所在安全组下不展示此安全组。

系统内置的安全组，无删除按钮。

# 运维中心（ECMC）

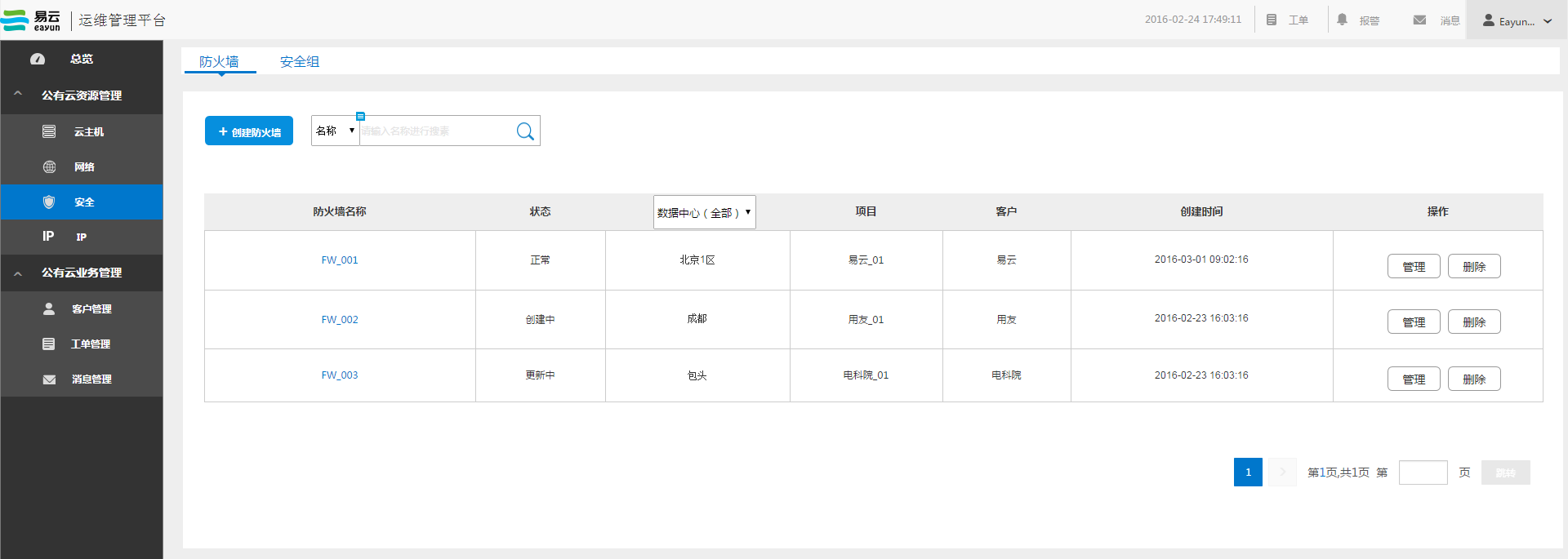
## 防火墙

### 查看防火墙

同管理控制台相比，运维平台需要调整功能如下：

* 1. 列表中需要增加“数据中心”、“项目”和“客户”三列；
  2. 数据中心（可下拉筛选）、名称、项目和客户查询功能作为通用功能，和ECMCv1.1保持一致；
  3. 防火墙列表展示所有数据中心下的防火墙记录，每页最多展示10条记录，超过10条则分页展示；

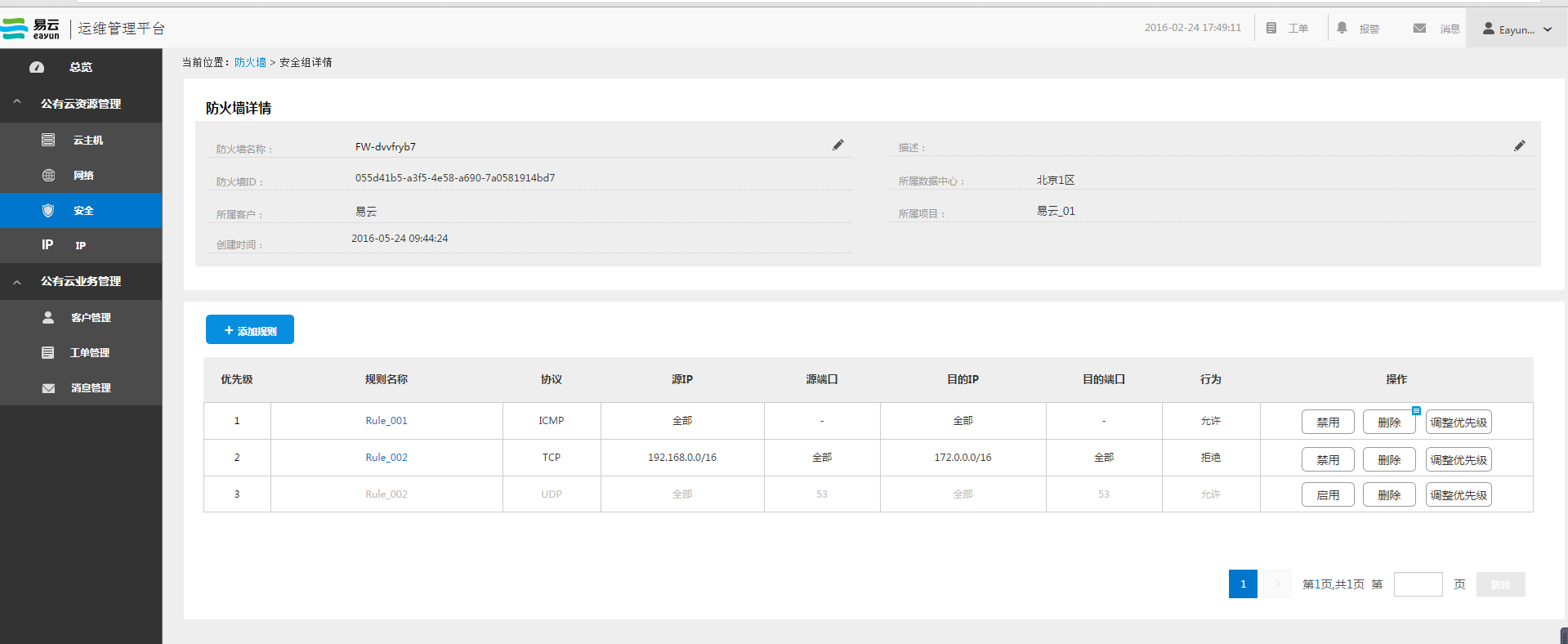
原型设计图如下所示：



图二十 防火墙列表页面\_ECMC

### 防火墙详情

同管理控制台相比，防火墙基本信息和防火墙规则详情中需要增加“所属客户”字段，同时基本信息中无“标签”字段，其他同管理控制台，原型示意如下：



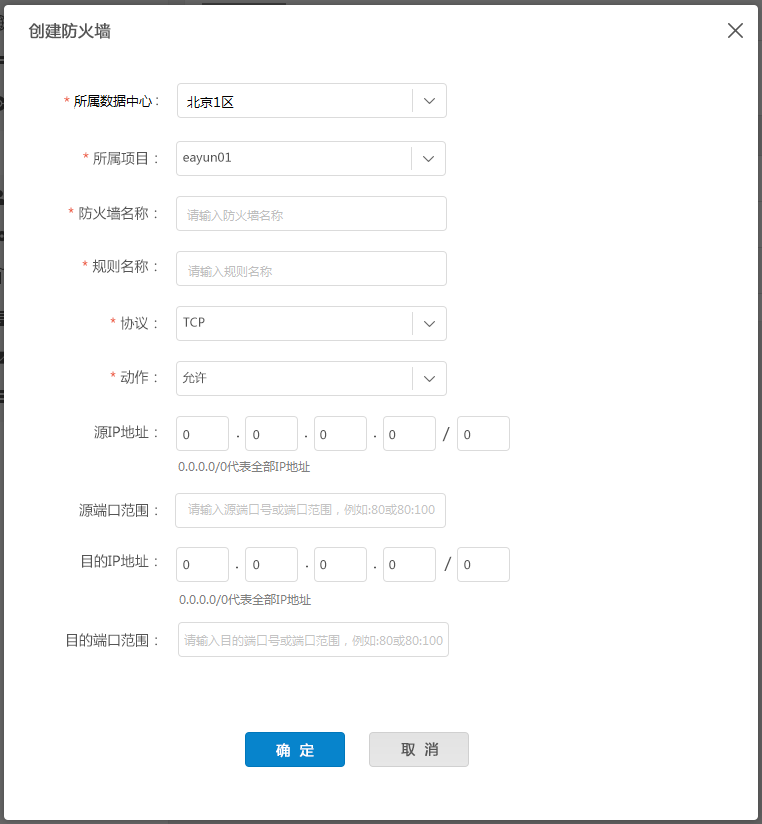
图二十一 防火墙详情页\_ECMC



图二十二 防火墙规则详情\_ECMC

### 创建防火墙

同管理控制台相比，创建防火墙页面需要增加“所属数据中心”，其原型设计如下：



图二十三 创建防火墙TCP/UDP\_ECMC



图二十四 创建防火墙ICMP/所有\_ECMC

### 更新防火墙

编辑防火墙、添加规则、禁用/启用规则、删除规则和调整优先级操作流程及界面展示同管理控制台（ECSC），详见“3.1.4.2**规则说明**”。

### 删除防火墙

点击删除按钮后，给出确认提示“删除后网络下的流量将不受限制，确定要删除防火墙XXX？” XXX指代防火墙名称，点击确定按钮后，执行删除操作，删除防火墙时会自动删除掉关联该防火墙的所有规则，同时后台也会删除默认生成的防火墙策略。

注：管理控制台中删除防火墙可以不显示对应的名称，运维中心是所有客户所有数据中心的资源集中管理，故为了防止出错，此处必须捎带防火墙名称。

## 安全组

### 查看安全组

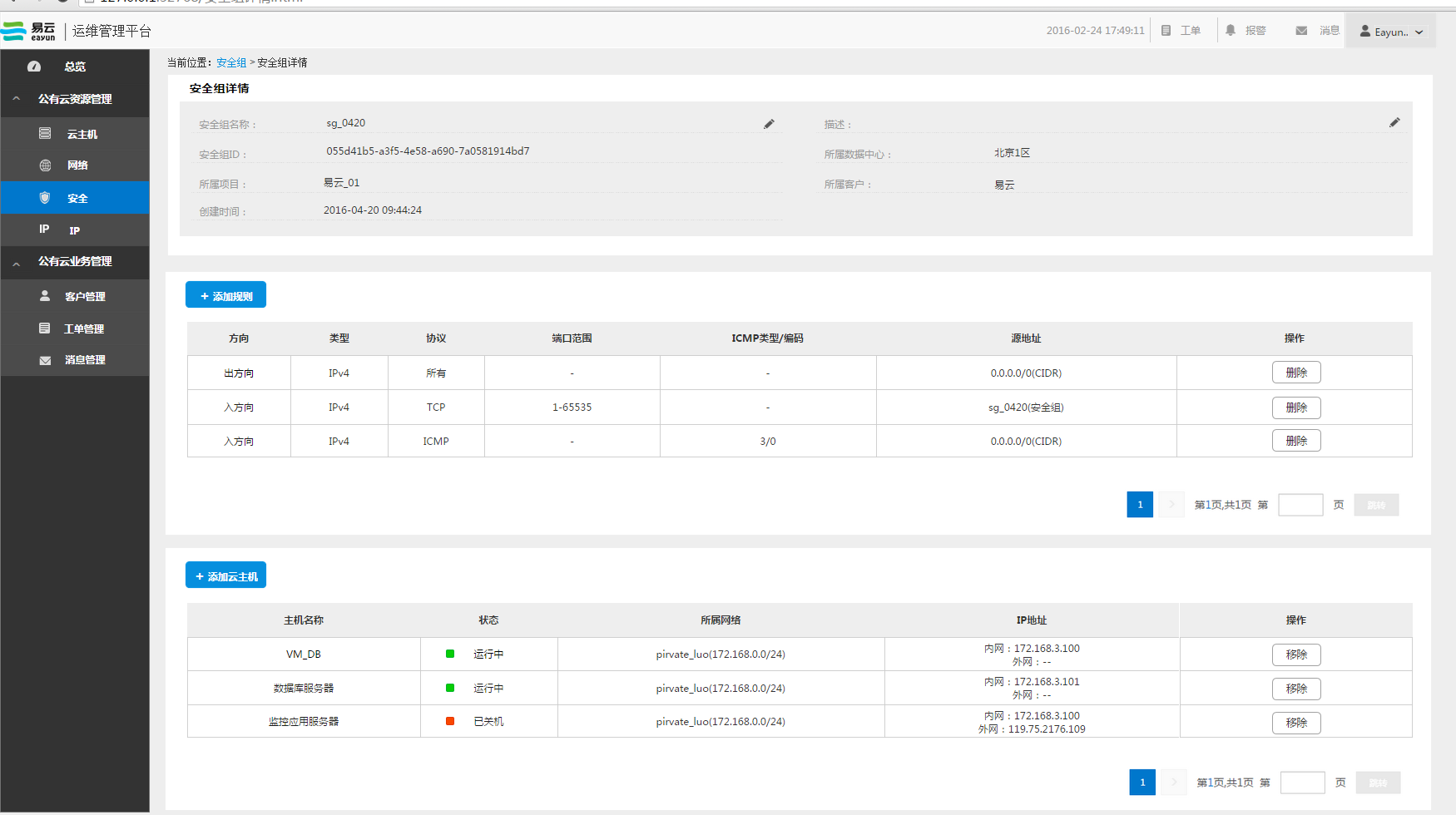
同运维平台ECMCv1.1相比，列表中需要增加“创建时间”列，同时操作列的按钮为“管理”和“删除”，其风格沿用ECMCv1.1，原型示意如下：



图二十五 安全组列表\_ECMC

### 安全组详情

同管理控制台（ECSC）相比，基本信息中需要加上“所属客户”字段，同时去掉“标签”字段，设计风格沿用ECMCv1.1，其原型示意如下：



图二十六 安全组详情\_ECMC

### 创建安全组

创建安全组同ECMCv1.0，界面不做调整，但是名称唯一性，从同一数据中心下修改为同一项目下唯一（同管理控制台一致）。

### 更新安全组

编辑安全组、添加/删除规则、添加/移除云主机功能同管理控制台（ECSC），见章节“3.2.4.2**规则描述**”

### 删除安全组

删除逻辑同管理控制台，此版本去掉安全组被云主机使用，则不允许删除的限定条件。

# 权限和日志

## ECSC

### 权限

表十一 安全模块权限表\_ECSC

| **序号** | **模块** | **功能点** | **超级管理员** | **管理员** | **普通用户** |
| --- | --- | --- | --- | --- | --- |
|  | 防火墙 | 查看 | Y | Y | Y |
|  | 创建 | Y | Y | N |
|  | 编辑 | Y | Y | N |
|  | 标签 | Y | Y | N |
|  | 添加规则 | Y | Y | N |
|  | 禁用规则 | Y | Y | N |
|  | 删除规则 | Y | Y | N |
|  | 调整优先级 | Y | Y | N |
|  | 删除防火墙 | Y | Y | N |
|  | 安全组 | 查看 | Y | Y | Y |
|  | 创建 | Y | Y | N |
|  | 编辑 | Y | Y | N |
|  | 标签 | Y | Y | N |
|  | 添加规则 | Y | Y | N |
|  | 删除规则 | Y | Y | N |
|  | 添加云主机 | Y | Y | N |
|  | 移除云主机 | Y | Y | N |
|  | 删除安全组 | Y | Y | N |

### 日志

表十二 安全模块日志记录信息\_ECSC

| 序号 | 操作项 | 资源类型 | 资源名称 | 说明 |
| --- | --- | --- | --- | --- |
|  | 创建防火墙 | 防火墙 | 防火墙名称 |  |
|  | 编辑防火墙 | 防火墙 | 防火墙名称 |  |
|  | 设置标签 | 防火墙 | 防火墙名称 |  |
|  | 添加规则 | 防火墙规则 | 防火墙规则名称 |  |
|  | 删除规则 | 防火墙规则 | 防火墙规则名称 |  |
|  | 禁用规则 | 防火墙规则 | 防火墙规则名称 |  |
|  | 调整优先级 | 防火墙规则 | 防火墙规则名称 |  |
|  | 删除防火墙 | 防火墙 | 防火墙名称 |  |
|  | 创建安全组 | 安全组 | 安全组名称 |  |
|  | 编辑安全组 | 安全组 | 安全组名称 |  |
|  | 设置标签 | 安全组 | 安全组名称 |  |
|  | 添加规则 | 安全组 | 安全组名称 |  |
|  | 删除规则 | 安全组 | 安全组名称 |  |
|  | 加入安全组 | 云主机 | 云主机名称 |  |
|  | 移除安全组 | 云主机 | 云主机名称 |  |
|  | 删除安全组 | 安全组 | 安全组名称 |  |

## ECMC

### 权限

表十三 安全模块可配置权限表\_ECMC

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **模块** | **权限功能项** | **说明** |
|  | 防火墙 | 查看 | 列表展现、查询及查看详情功能 |
|  | 创建 | 创建防火墙同时添加规则 |
|  | 编辑 | 修改防火墙名称和描述 |
|  | 标签 | 防火墙设置标签 |
|  | 添加规则 | 防火墙中添加规则 |
|  | 禁用规则 | 禁用防火墙的规则 |
|  | 删除规则 | 删除防火墙中的规则 |
|  | 调整优先级 | 调整防火墙规则中的优先级 |
|  | 删除防火墙 | 删除防火墙 |
|  | 安全组 | 查看 | 列表展现、查询及查看详情功能 |
|  | 创建 | 创建安全组 |
|  | 编辑 | 修改安全组名称和描述 |
|  | 标签 | 安全组设置标签 |
|  | 添加规则 | 安全组中添加规则 |
|  | 删除规则 | 安全组中删除规则 |
|  | 添加云主机 | 安全组中添加云主机 |
|  | 移除云主机 | 安全组中移除云主机 |
|  | 删除安全组 | 删除安全组 |

表十四 安全模块内置角色预置权限表

| **序号** | **模块** | **功能点** | **管理员** | **运维** | **客服** | **商务** |
| --- | --- | --- | --- | --- | --- | --- |
|  | 防火墙 | 查看 | Y | Y | N | N |
|  | 创建 | Y | Y | N | N |
|  | 编辑 | Y | Y | N | N |
|  | 标签 | Y | Y | N | N |
|  | 添加规则 | Y | Y | N | N |
|  | 禁用规则 | Y | Y | N | N |
|  | 删除规则 | Y | Y | N | N |
|  | 调整优先级 | Y | Y | N | N |
|  | 删除防火墙 | Y | Y | N | N |
|  | 安全组 | 查看 | Y | Y | N | N |
|  | 创建 | Y | Y | N | N |
|  | 编辑 | Y | Y | N | N |
|  | 标签 | Y | Y | N | N |
|  | 添加规则 | Y | Y | N | N |
|  | 删除规则 | Y | Y | N | N |
|  | 添加云主机 | Y | Y | N | N |
|  | 移除云主机 | Y | Y | N | N |
|  | 删除安全组 | Y | Y | N | N |

### 日志

表十五 安全模块操作日志记录信息\_ECMC

| 序号 | 操作项 | 资源类型 | 资源名称 | 资源ID | 说明 |
| --- | --- | --- | --- | --- | --- |
|  | 创建防火墙 | 防火墙 | 防火墙名称 | 防火墙ID |  |
|  | 编辑防火墙 | 防火墙 | 防火墙名称 | 防火墙ID |  |
|  | 设置标签 | 防火墙 | 防火墙名称 | 防火墙ID |  |
|  | 添加规则 | 防火墙规则 | 防火墙规则名称 | 防火墙规则ID |  |
|  | 删除规则 | 防火墙规则 | 防火墙规则名称 | 防火墙规则ID |  |
|  | 禁用规则 | 防火墙规则 | 防火墙规则名称 | 防火墙规则ID |  |
|  | 调整优先级 | 防火墙规则 | 防火墙规则名称 | 防火墙规则ID |  |
|  | 删除防火墙 | 防火墙 | 防火墙名称 | 防火墙ID |  |
|  | 创建安全组 | 安全组 | 安全组名称 | 安全组ID |  |
|  | 编辑安全组 | 安全组 | 安全组名称 | 安全组ID |  |
|  | 设置标签 | 安全组 | 安全组名称 | 安全组ID |  |
|  | 添加规则 | 安全组 | 安全组名称 | 安全组ID |  |
|  | 删除规则 | 安全组 | 安全组名称 | 安全组ID |  |
|  | 加入安全组 | 云主机 | 云主机名称 | 云主机ID |  |
|  | 移除安全组 | 云主机 | 云主机名称 | 云主机ID |  |
|  | 删除安全组 | 安全组 | 安全组名称 | 安全组ID |  |