  
Neutron 默认的安全组规则会禁止掉所有从外面访问 instance 的流量。

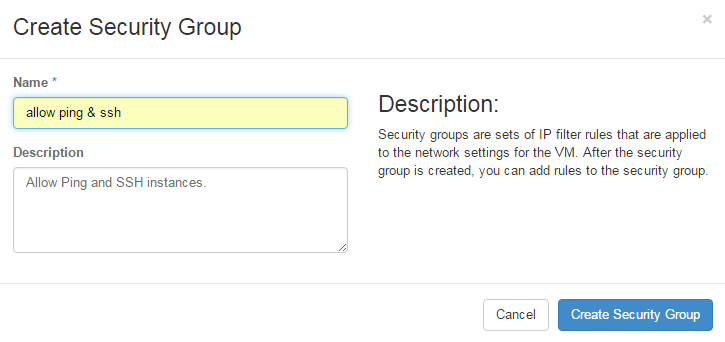
本节我们会修改安全组的配置，允许 ping 和 ssh instance。  
有两种方法可以达到这个目的：

1. 修改 “default” 安全组。

2. 为 cirros-vm1 添加新的安全组。

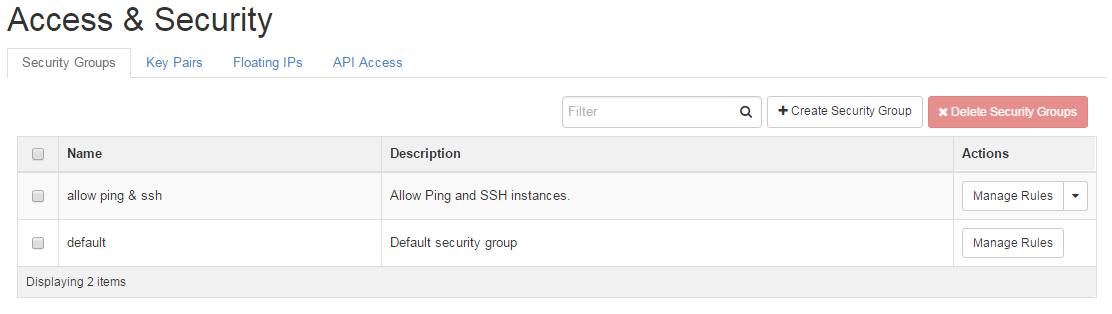
这里我们采用第二种方法。

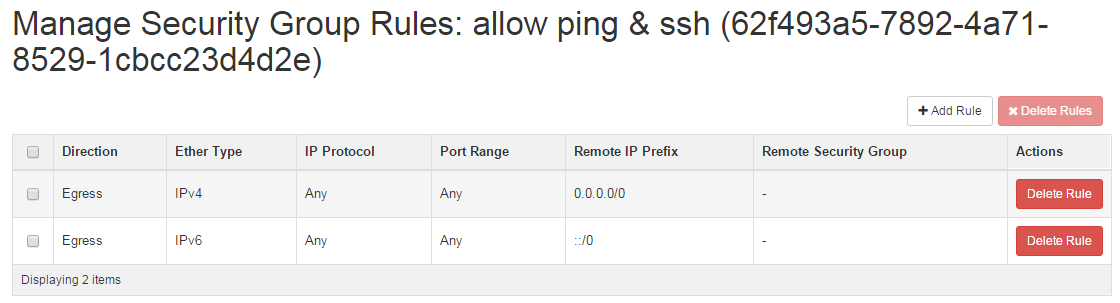
在安全组列表页面点击http://7xo6kd.com1.z0.glb.clouddn.com/upload-ueditor-image-20161122-1479770555033099510.jpg按钮。



为安全组命名并点击 “Create Security Group”。

新的安全组 “allow ping & ssh” 创建成功。

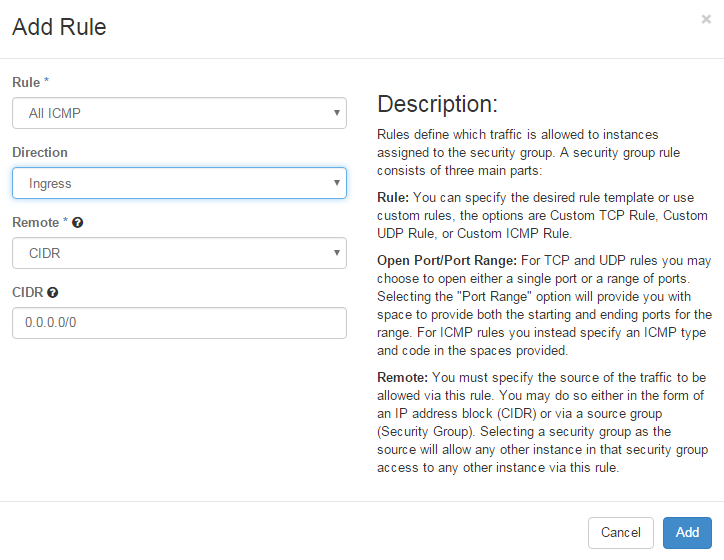


点击http://7xo6kd.com1.z0.glb.clouddn.com/upload-ueditor-image-20161122-1479770555472081965.jpg按钮，查看 “allow ping & ssh” 的规则。  


系统默认定义了两条规则，运行所有的外出流量。

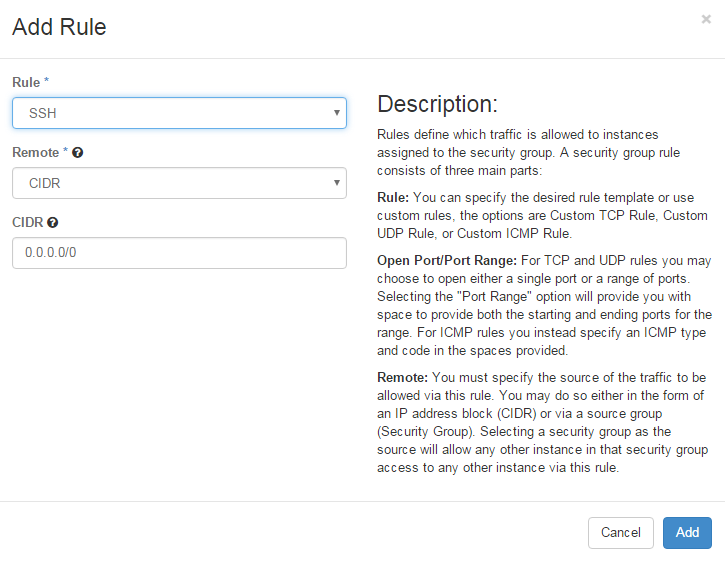
为清晰起见，可以点击http://7xo6kd.com1.z0.glb.clouddn.com/upload-ueditor-image-20161122-1479770555708097973.jpg按钮删除这两条规则。

点击http://7xo6kd.com1.z0.glb.clouddn.com/upload-ueditor-image-20161122-1479770555810068838.jpg按钮，添加允许 ping 的规则。

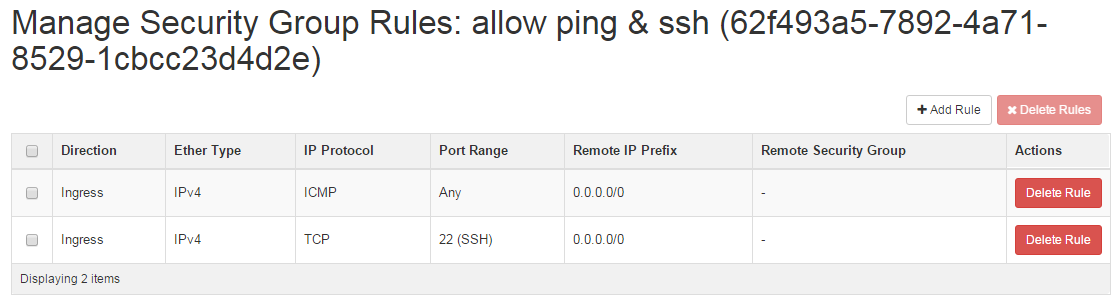


“Rule” 选择 “All ICMP”，“Direction” 选择 “Ingress”，然后点击 “Add” 按钮。

同样的方式添加 ssh 规则。

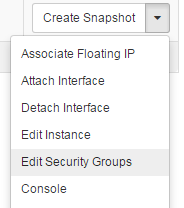


在列表中查看添加成功的规则。

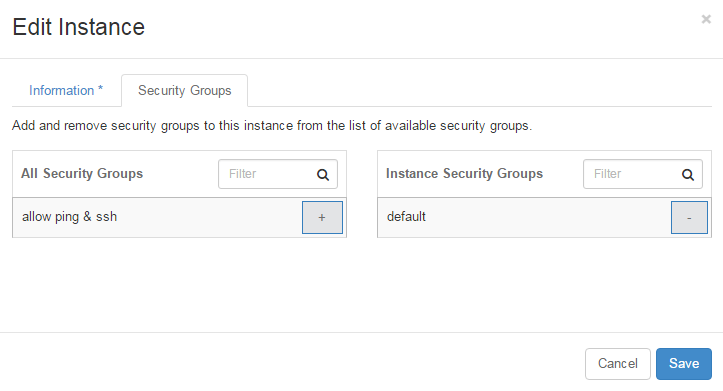


接下来设置 cirros-vm1，使用新的安全组。

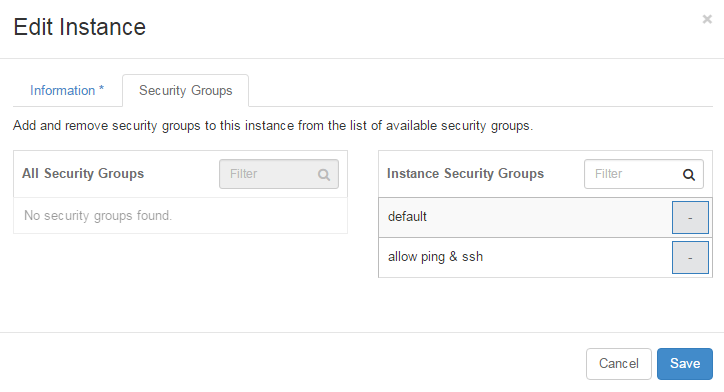
进入 instance 列表页面，点击 cirros-vm1 下拉操作列表中的 “Edit Security Groups”



可以看到 cirros-vm1 当前使用的安全组为 “default”，可选安全组为 “allow ping & ssh”。

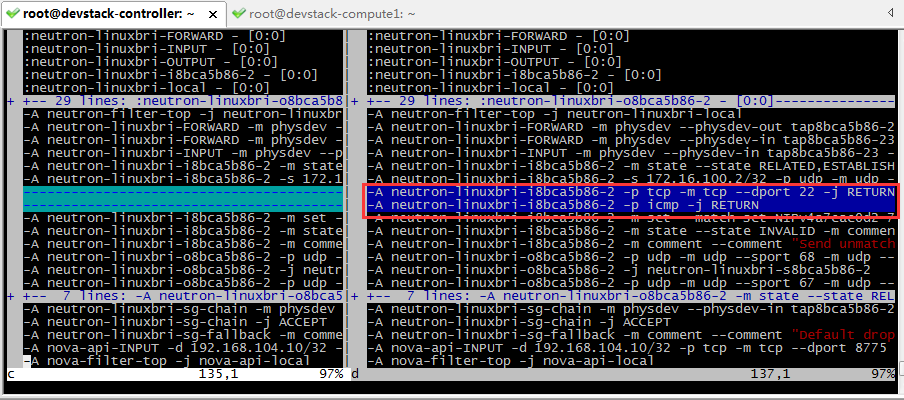


点击安全组 “allow ping & ssh” 后面的 “+” 按钮。



点击 “Save” 保存。

iptables 会立即更新，下面通过 vimdiff 查看 iptables 前后的变化。



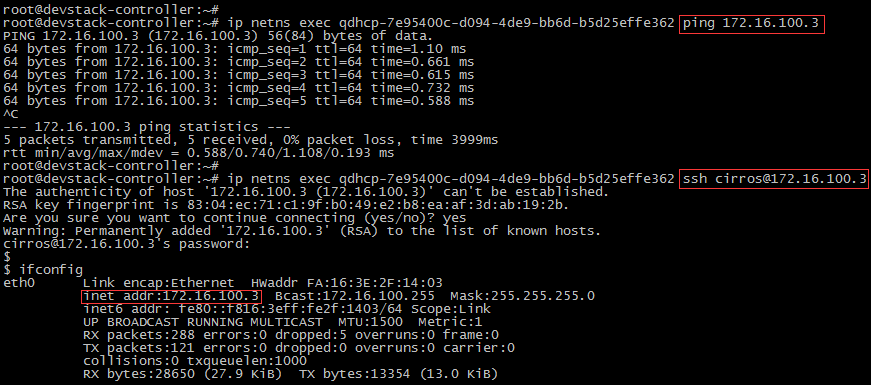
“allow ping & ssh” 安全组引入了下面两条 iptables 规则。

作用是运行 ingress 的 ssh 和 ping 流量。

-A neutron-linuxbri-i8bca5b86-2 -p tcp -m tcp --dport 22 -j RETURN

-A neutron-linuxbri-i8bca5b86-2 -p icmp -j RETURN

测试一下，现在能够 ping 和 ssh cirros-vm1 了。



**小结**

安全组有以下特性：

1. 通过宿主机上 iptables 规则控制进出 instance 的流量。

2. 安全组作用在 instance 的 port 上。

3. 安全组的规则都是 allow，不能定义 deny 的规则。

4. instance 可应用多个安全组叠加使用这些安全组中的规则。

安全组学习完了，下节我们讨论 Neutron 的另一个安全机制 -- 虚拟防火墙。