(19)中华人民共和国国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 112688913 A
(43)申请公布日 2021.04.20

(21)申请号 202011342708.7

(22)申请日 2020.11.25

(71)申请人 紫光云技术有限公司
地址 300459 天津市滨海新区高新区塘沽海洋科技园汇祥道399号6号楼

(72)发明人 范生越

(74)专利代理机构 天津滨海科纬知识产权代理有限公司 12211
代理人 杨正律

(51)Int.Cl.
H04L 29/06(2006.01)
G06F 9/455(2006.01)

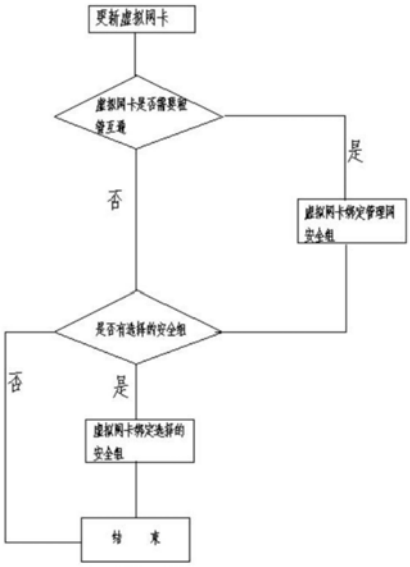
权利要求书1页 说明书4页 附图2页

(54)发明名称

一种OpenStack安全组优化方法

(57)摘要

本发明提供了一种OpenStack安全组优化方法，租户自己创建自定义安全组，租户开通自动创建一个管理网安全组、租户进行购买指令、虚拟网卡更新，购买指令传递到控制层，控制层将信息传递给OpenStack的Neutron层、租户开始选择安全组、Openstack层攒好的配置通过agent的driver驱动下发到物理设备上，本发明所述的一种OpenStack安全组优化方法，有OpenStack上面的控制层来控制所有安全组的操作，虚拟机的安全性更高，租管互通是PaaS类产品的内部操作，租管互通需要放行的IP地址，租户不感知，利用管理网安全组自动绑定虚拟机，满足租管互通的放行管理网IP地址需求，管理网安全组的安全组规则放行的IP地址可控、灵活性高。



CN 112688913 A

1.一种OpenStack安全组优化方法,其特征在于:包括以下步骤

S1:租户自己创建自定义安全组,租户开通自动创建一个管理网安全组;

S2:租户进行购买指令;

S3:虚拟网卡更新,购买指令传递到控制层,控制层需要根据租户购买的产品类型来判断虚拟机是否需要使用租管互通,放行管理网地址,将信息传递给OpenStack的Neutron层;

S4:Neutron层根据控制层传递的信息,若虚拟机绑定安全组时需要使用租管互通,则自动将管理网安全组与虚拟机绑定,储存绑定关系,待虚拟机删除时,将虚拟机与管理网安全组进行解绑操作,自动将管理网安全组与虚拟机绑定之后进行步骤S5,若不需要用租管互通,租户则直接进行步骤S5;

S5:租户开始选择安全组,若没有选择的安全组则直接进行步骤S6,然后进行步骤S6,若有选择的安全组,租户则自行选择之前租户创建的自定义安全组,自定义安全组与虚拟机绑定,绑定之后进行步骤S6;

S6:Openstack层攒好的配置通过agent的driver驱动下发到物理设备上。

2.根据权利要求1所述的一种OpenStack安全组优化方法,其特征在于:所述管理网安全组在出方向和入方向上放行需要放行的管理网IP地址,此管理网安全组所有租户共用。

3.根据权利要求1所述的一种OpenStack安全组优化方法,其特征在于:所述租管互通需要安全组将管理网放行。

4.根据权利要求1所述的一种OpenStack安全组优化方法,其特征在于:所述租管互通是PaaS类产品的内部操作。

5.根据权利要求1所述的一种OpenStack安全组优化方法,其特征在于:所述租管互通需要放行IP地址,管理网安全组是租户不可见、不感知的。

6.根据权利要求1所述的一种OpenStack安全组优化方法,其特征在于:所述自定义安全组是租户可见、可感知的。

7.根据权利要求1所述的一种OpenStack安全组优化方法,其特征在于:所述OpenStack上面的控制层来控制所有安全组的操作。

一种OpenStack安全组优化方法

技术领域

[0001] 本发明属于云计算与虚拟化领域,尤其是涉及一种OpenStack安全组优化方法。

背景技术

[0002] OpenStack Neutron为ECS实例提供了两种网络安全方式:安全组和虚拟防火墙。安全组的原理是利用iptables对ECS实例所在的计算节点的网络流量进行过滤,虚拟防火墙底层也是通过iptables在Router上对网络报文进行过滤。安全组具有状态检测和数据包过滤的能力,在云计算领域,利用安全组在云端划分安全域,通过设置安全组规则来实现控制安全组内ECS实例的入流量和出流量;OpenStack中提供的安全组方案,每一个租户都会自动创建一个命名为default的默认安全组,使用default安全组的虚拟机允许向外部发送数据报文,但禁止所有外部流量进入虚拟机(两个ECS实例使用同一个default安全组除外),租户在创建ECS实例时如果未创建新的安全组,则会被强制使用default安全组;

[0003] 租户在创建ECS虚拟机实例时,如果除了default安全组没有其他自建的安全组可供选择,则会被强制使用default安全组,但是default安全组有以下几个弊端:

[0004] default安全组规则全部放行,存在安全风险;

[0005] 一些依赖ECS虚拟机的PaaS类产品,如RDS数据库,容器,KAFKA等产品,租户在购买这个产品后,由于这些产品要依赖虚拟机来实现,如果要做高可用就需要更多的虚拟机,这些虚拟机都会使用default安全组,但是租户对这些产品支撑所用的虚拟机并不感知,一旦default安全组规则有改动,则会影响这些产品的正常使用;

[0006] 由于很多场景的需求,有些产品要实现租户网与管理网的互通(以下简称租管互通),租管互通需要打通管理网与租户网之间的通讯壁垒,进入虚拟机的流量不能完全被禁止,来自管理网的流量报文需要进入虚拟机,使用default安全组的虚拟机就会将管理网的流量过滤掉,就不能满足租管互通的需求。

发明内容

[0007] 有鉴于此,本发明旨在提出一种OpenStack安全组优化方法,以解决default安全组固有的限制性问题。

[0008] 为达到上述目的,本发明的技术方案是这样实现的:

[0009] 一种OpenStack安全组优化方法,包括以下步骤

[0010] S1:租户自己创建自定义安全组,租户开通自动创建一个管理网安全组;

[0011] S2:租户进行购买指令;

[0012] S3:虚拟网卡更新,购买指令传递到控制层,控制层需要根据租户购买的产品类型来判断虚拟机是否需要使用租管互通,放行管理网地址,将信息传递给OpenStack的Neutron层;

[0013] S4:Neutron层根据控制层传递的信息,若虚拟机绑定安全组时需要使用租管互通,则自动将管理网安全组与虚拟机绑定,储存绑定关系,待虚拟机删除时,将虚拟机与管

理网安全组进行解绑操作，自动将管理网安全组与虚拟机绑定之后进行步骤S5，若不需要用租管互通，租户则直接进行步骤S5；

[0014] S5：租户开始选择安全组，若没有选择的安全组则直接进行步骤S6，然后进行步骤S6，若有选择的安全组，租户则自行选择之前租户创建的自定义安全组，自定义安全组与虚拟机绑定，绑定之后进行步骤S6；

[0015] S6：Openstack层攒好的配置通过agent的driver驱动下发到物理设备上

[0016] 进一步的，所述管理网安全组在出方向和入方向上放行需要放行的管理网IP地址，此管理网安全组所有租户共用。

[0017] 进一步的，所述租管互通需要安全组将管理网放行。

[0018] 进一步的，所述租管互通是PaaS类产品的内部操作。

[0019] 进一步的，所述租管互通需要放行IP地址，管理网安全组是租户不可见、不感知的。

[0020] 进一步的，所述自定义安全组是租户可见、可感知的。

[0021] 进一步的，所述OpenStack上面的控制层来控制所有安全组的操作。

[0022] 相对于现有技术，本发明所述的一种OpenStack安全组优化方法具有以下优势：

[0023] (1)本发明所述的一种OpenStack安全组优化方法，主要有两个方面的修改，一是将default安全组在Neutron中移除，有OpenStack上面的控制层来控制所有安全组的操作，虚拟机的安全性更高，不再使用OpenStack自带的default安全组，虚拟机出方向和入方向流量默认全部禁止，对于虚拟机安全性更高，删除default安全组后，虚拟机的安全性更高，且租户所有的安全组完全自主可控；二是租管互通需要安全组将管理网放行，租管互通是PaaS类产品的内部操作，租管互通需要放行的IP地址，租户不感知，利用管理网安全组自动绑定虚拟机，满足租管互通的放行管理网IP地址需求，管理网安全组的安全组规则放行的IP地址可控、灵活性高，本发明需要创建一个管理网安全组，安全组规则中放行租管互通的IP地址，再将管理网安全组与虚拟机自动绑定，达到放行管理网IP的目的。

附图说明

[0024] 构成本发明的一部分的附图用来提供对本发明的进一步理解，本发明的示意性实施例及其说明用于解释本发明，并不构成对本发明的不当限定。在附图中：

[0025] 图1为本发明实施例所述的一种OpenStack安全组优化的结构图；

[0026] 图2为本发明实施例所述的OpenStack Neutron部分的流程图。

具体实施方式

[0027] 需要说明的是，在不冲突的情况下，本发明中的实施例及实施例中的特征可以相互组合。

[0028] 在本发明的描述中，需要理解的是，术语“中心”、“纵向”、“横向”、“上”、“下”、“前”、“后”、“左”、“右”、“竖直”、“水平”、“顶”、“底”、“内”、“外”等指示的方位或位置关系为基于附图所示的方位或位置关系，仅是为了便于描述本发明和简化描述，而不是指示或暗示所指的装置或元件必须具有特定的方位、以特定的方位构造和操作，因此不能理解为对本发明的限制。此外，术语“第一”、“第二”等仅用于描述目的，而不能理解为指示或暗示相

对重要性或者隐含指明所指示的技术特征的数量。由此，限定有“第一”、“第二”等的特征可以明示或者隐含地包括一个或者更多个该特征。在本发明的描述中，除非另有说明，“多个”的含义是两个或两个以上。

[0029] 在本发明的描述中，需要说明的是，除非另有明确的规定和限定，术语“安装”、“相连”、“连接”应做广义理解，例如，可以是固定连接，也可以是可拆卸连接，或一体地连接；可以是机械连接，也可以是电连接；可以是直接相连，也可以通过中间媒介间接相连，可以是两个元件内部的连通。对于本领域的普通技术人员而言，可以通过具体情况理解上述术语在本发明中的具体含义。

[0030] 下面将参考附图并结合实施例来详细说明本发明。

[0031] 名词解释：

[0032] Neutron是OpenStack项目中负责提供网络服务的组件，它基于软件定义网络的思想，实现了网络虚拟化下的资源管理。

[0033] ECS(Elastic Compute Service，云服务器)是一种简单高效、安全可靠、处理能力可弹性伸缩的计算服务。

[0034] OpenStack是一个开源的云计算管理平台项目，是一系列软件开源项目的组合。

[0035] PaaS是(Platform as a Service)的缩写，是指平台即服务。把服务器平台作为一种服务提供的商业模式，通过网络进行程序提供的服务称之为SaaS(Software as a Service)，而云计算时代相应的服务器平台或者开发环境作为服务进行提供就成为了PaaS(Platform as a Service)。

[0036] IPTABLES是与最新的3.5版本Linux内核集成的IP信息包过滤系统。

[0037] RDS是关系型数据库服务(Relational Database Service)的简称，是一种即开即用、稳定可靠、可弹性伸缩的在线数据库服务。

[0038] driver是给硬件设备下配置的。

[0039] 默认安全组：即default安全组，default安全组也是默认安全组。。

[0040] 如图1-2所示，一种OpenStack安全组优化方法包括以下步骤：

[0041] S1：租户自己创建自定义安全组，自定义安全组供租户在之后自己选择安全组的时候选择，租户开通自动创建一个管理网安全组，管理网安全组的安全组规则放行的IP地址可控、灵活性高，设置管理网安全组，安全组规则放行管理网IP地址，租户既不感知，又满足了PaaS类产品对于放行管理网IP的需求；

[0042] S2：租户进行购买指令；

[0043] S3：虚拟网卡更新，购买指令传递到控制层，控制层需要根据租户购买的产品类型来判断虚拟机是否需要使用租管互通，放行管理网地址，将信息传递给OpenStack的Neutron层，因为租管互通需要放行IP地址；

[0044] S4：Neutron层根据控制层传递的信息，若虚拟机绑定安全组时需要使用租管互通，则自动将管理网安全组与虚拟机绑定，储存绑定关系，待虚拟机删除时，将虚拟机与管理网安全组进行解绑操作，自动将管理网安全组与虚拟机绑定之后进行步骤S5，便于实现租管互通，若不需要用租管互通，租户则直接进行步骤S5；

[0045] S5：租户开始选择安全组，若没有选择的安全组则直接进行步骤S6，然后进行步骤S6，若有选择的安全组，租户则自行选择之前租户创建的自定义安全组，自定义安全组与虚

拟机绑定,绑定之后进行步骤S6,租户有一定的选择权利,提高了灵活性;

[0046] S6:Openstack层攒好的配置通过agent的driver驱动下发到物理设备上;

[0047] 所述管理网安全组在出方向和入方向上放行需要放行的管理网IP地址,此管理网安全组所有租户共用;所述租管互通需要安全组将管理网放行;所述租管互通是PaaS类产品的内部操作;所述租管互通需要放行IP地址,管理网安全组是租户不可见、不感知的,管理网安全组的安全组规则放行的IP地址可控、灵活性高;所述自定义安全组是租户可见、可感知的;所述OpenStack上面的控制层来控制所有安全组的操作,虚拟机的安全性更高。

[0048] 以上所述仅为本发明的较佳实施例而已,并不用以限制本发明,凡在本发明的精神和原则之内,所作的任何修改、等同替换、改进等,均应包含在本发明的保护范围之内。

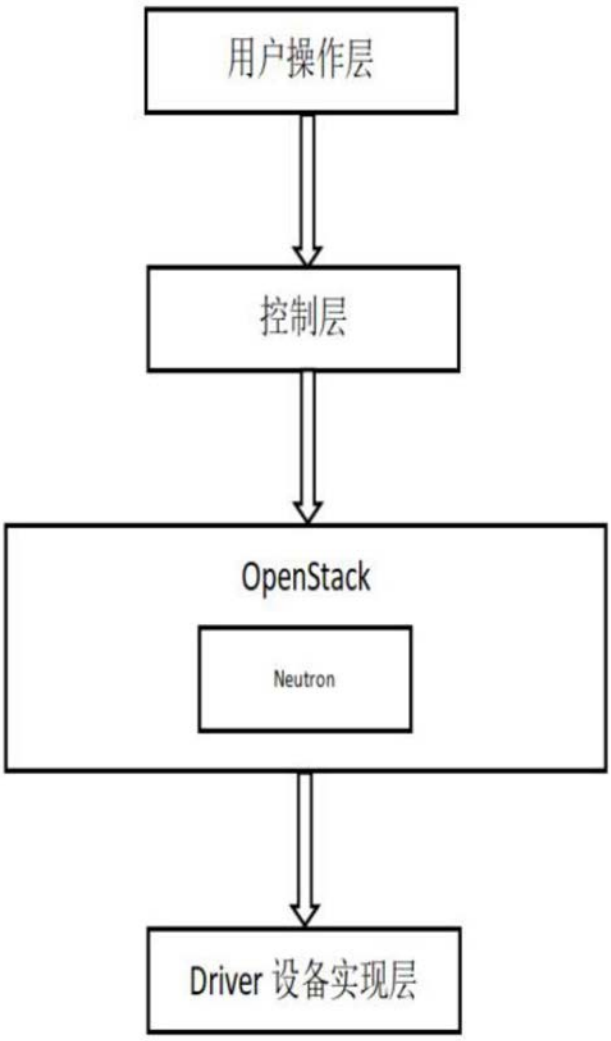


图1

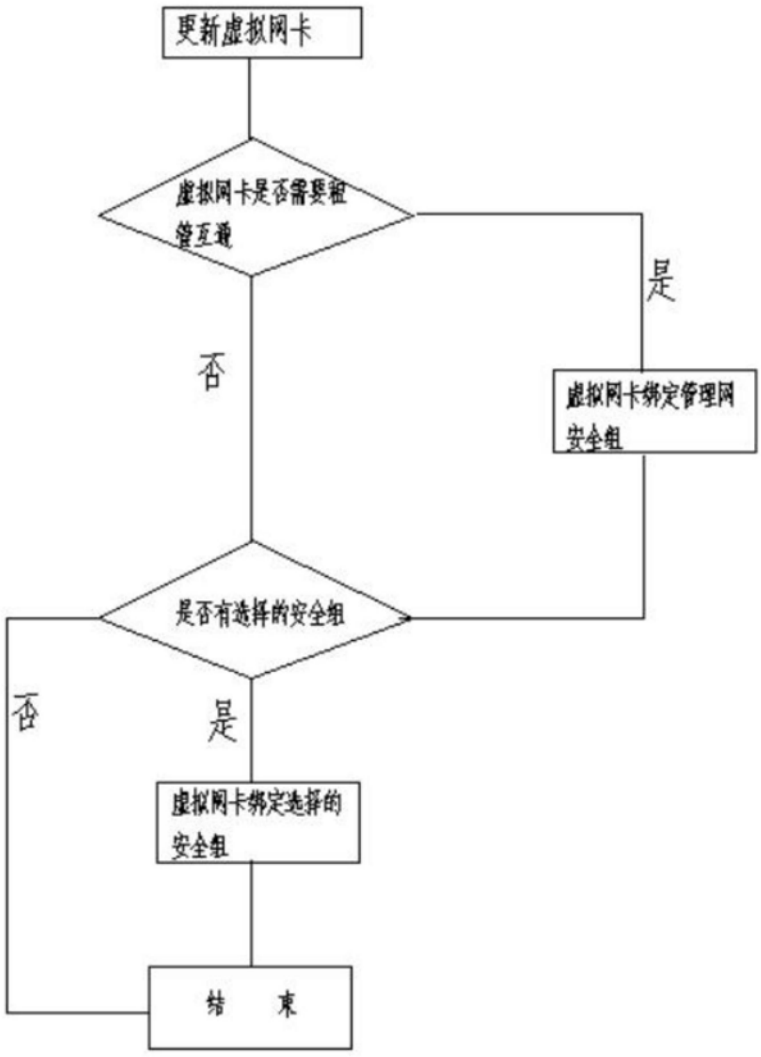

更新虚拟网卡
虚拟网卡是否需要和
管互通
是
否
虚拟网卡绑定管理网
安全组
是否有选择的安全组
否
是
虚拟网卡绑定选择的
安全组
结 束

图2