(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 111131212 A
(43)申请公布日 2020.05.08

(21)申请号 201911306787.3

(22)申请日 2019.12.17

(71)申请人 紫光云(南京)数字技术有限公司
地址 210000 江苏省南京市浦口区江浦街道浦滨路320号浦口科创广场科创总部大厦B座17楼

(72)发明人 李明泽

(51)Int.Cl.
H04L 29/06(2006.01)
H04L 29/08(2006.01)

权利要求书1页 说明书2页

(54)发明名称

一种基于OpenStack绑定安全组方法

(57)摘要

本发明提供了一种基于OpenStack绑定安全组方法,预先在各个机房创建对应后台管理的网安全组,定义流量放行的策略;改写OpenStack中创建、修改安全组的API,增加新的接口参数is_visible,用以标识安全组是否可见;在neutron DB中增加持久化安全组规则is_visible的表结构;修改port与安全组绑定的方法,在完成原有的绑定逻辑后,再额外将对应后台管理的网安全组绑定到该port上;修改port的查询和列表接口,过滤掉字段中is_visible=false的安全组。本发明用于为云主机绑定后台安全组,可以为管理网的流量放行,同时避免用户修改。

CN 111131212 A

1.一种基于OpenStack绑定安全组方法,其特征在于修改原生的安全组API增加新属性,在port绑定其他安全组的同时将我们的对应后台管理的网安全组绑定到该port上,并且在port的查询和列表接口,对不可见的安全组进行处理。

2.根据权利要求1所述的基于OpenStack绑定安全组方法,其特征在于包括如下步骤:

(1)预先在各个机房创建对应后台管理的网安全组,并根据各个机房的管理网IP地址,在安全组中创建对应的安全组规则,定义流量放行的策略;

(2)改写OpenStack中创建、修改安全组的API,增加新的接口参数is_visible,用以标识安全组是否可见,其中默认true表示可见,false表示不可见;并在安全组查询或列表接口中增加对该字段的条件判断,默认返回is_visible=true的安全组;

(3)在neutron DB中增加持久化安全组规则is_visible的表结构;

(4)修改port与安全组绑定的方法,在完成原有的绑定逻辑后,再额外将对应后台管理的网安全组绑定到该port上;

(5)修改port的查询和列表接口,过滤掉字段中is_visible=false的安全组。

3.根据权利要求2所述的基于OpenStack绑定安全组方法,其特征在于上述步骤(2)中的OpenStack是一个为公共及私有云的建设与管理提供软件的开源项目,OpenStack作为基础设施即服务资源的通用前端。

一种基于OpenStack绑定安全组方法

技术领域

[0001] 本发明涉及基于OpenStack绑定安全组方法的技术领域。

背景技术

[0002] OpenStack经过长期以来的不断迭代与优化,已经成为云计算领域重要的一部分,众多公有云和私有云厂商都会基于OpenStack进行二次开发进而输出云服务,但是原生的OpenStack实现商业化应用还有很多工作需要完善,绑定安全组就有如下一个特殊场景。

[0003] 现有的OpenStack绑定安全组,调用的是port的create或update接口,在接口的参数security_groups中设定或变更绑定的安全组。这样绑定的安全组,可以在port列表接口中被用户查询到或更改,这是正常而又单纯的使用场景,也是没有问题的。但是实际生产环境中,会有一些特殊场景,需要为用户的虚拟网卡(或者云主机)绑定安全组并在组内定义一些规则,并且不希望用户有所感知,更不希望用户查询到被绑定的安全组甚至去解绑安全组或者修改组内的规则。

[0004] 例如,一般公有云集群内的网络会划分成租户网络和管理网络或某类专有网络,一些用户的所使用的服务会依赖用户所在租户网络以外的服务的支撑,比如租户使用的LB(负载均衡)服务会依赖管理网中LB健康监测服务,这时候就需要为用户LB下挂载的实例放开LB健康监测服务流量访问,即配置安全组对应的规则将流量放行,而这样的安全组规则是不需要用户感知的,更不希望用户对组内的规则进行修改或误操作,以免服务不可用。

[0005] 因此,作为公有云服务商,有必要在用户不感知的情况下,默认绑定一个用户不感知(即不可见的)安全组,放行基础服务的访问流量,以便更灵活的实现自身的产品功能,并更好更稳定的为用户提供的产品支撑。

发明内容

[0006] 本发明的基于OpenStack绑定安全组方法,在原生的OpenStack中,提出一种用户无感知的方法,用于为云主机绑定后台安全组,可以为管理网的流量放行,同时避免用户修改。

[0007] 基于OpenStack绑定安全组方法,修改原生的安全组API增加新属性,在port绑定其他安全组的同时将我们的对应后台管理的网安全组绑定到该port上,并且在port的查询和列表接口,对不可见的安全组进行处理。

[0008] 本发明的基于OpenStack绑定安全组方法,具体包括如下步骤:

[0009] (1)预先在各个机房创建对应后台管理的网安全组,并根据各个机房的管理网IP地址,在安全组中创建对应的安全组规则,定义流量放行的策略;

[0010] (2)改写OpenStack中创建、修改安全组的API,增加新的接口参数is_visible,用以标识安全组是否可见,其中默认true表示可见,false表示不可见;并在安全组查询或列表接口中增加对该字段的条件判断,默认返回is_visible=true的安全组;

[0011] (3)在neutron DB中增加持久化安全组规则is_visible的表结构;

[0012] (4)修改port与安全组绑定的方法,在完成原有的绑定逻辑后,再额外将对应后台管理的网安全组绑定到该port上;

[0013] (5)修改port的查询和列表接口,过滤掉字段中is_visible=false的安全组。

[0014] 本发明的OpenStack是一个为公共及私有云的建设与管理提供软件的开源项目,OpenStack作为基础设施即服务资源的通用前端。

[0015] 本发明在用户不感知的情况下,默认绑定一个用户不感知(即不可见的)安全组,放行基础服务的访问流量,以便更灵活的实现自身的产品功能,并同时避免用户修改该安全组,可以更好更稳定的为用户提供的产品支撑。

具体实施方式

[0016] 基于OpenStack绑定安全组方法,为了实现用户无感知的绑定安全组,我们需要修改原生的安全组API增加新属性,同时在port绑定其他安全组的同时也将我们的对应后台管理的网安全组绑定到该port上,并且在port的查询和列表接口,对不可见的安全组进行处理。具体需要分以下几个步骤实现:

[0017] (1)预先在各个机房创建对应后台管理的网安全组,并根据各个机房的不通管理网IP地址,在安全组中创建对应的安全组规则,定义流量放行的策略;

[0018] (2)改写OpenStack中创建、修改安全组的API,增加新的接口参数is_visible,用以标识安全组是否可见,其中true表示可见(默认值),false表示不可见;并在安全组查询或列表接口中增加对该字段的条件判断(默认返回is_visible=true的安全组);

[0019] (3)在neutron DB中增加持久化安全组规则is_visible的表结构;

[0020] (4)修改port与安全组绑定的方法,在完成原有的绑定逻辑后,再额外将对应后台管理的网安全组绑定到该port上;

[0021] (5)修改port的查询和列表接口,因为该接口的security_groups中会返回该port绑定安全组信息,此时则需要从中过滤掉字段中is_visible=false的安全组,以此达到用户不可见不感知的目的,防止用户修改或解绑等误操作。

[0022] 本发明的系统架构为:

[0023] 为了实现用户无感知的绑定安全组,需要自顶向下修改云计算中网络模块所涉及的各个系统,包括:

[0024] 云计算管理控制台系统:面向用户来管理该用户的云计算资源,包括可视化页面和后台服务,在本发明中用于为用户提供创建、查询等安全组的入口界面,此次需要在向下调用neutron的时候对于新增加的参数is_visible不传值或者传值为true,以确保控制台层处理或获取的安全组中没有不可见的安全组。

[0025] OpenStack网络管理组件Neutron:云计算资源管理与调度层的工具,在本发明中该系统提供了安全组的增删改查接口和port与安全组的展示与绑定接口,并将结果持久化到数据库中。

[0026] 计算节点:云主机的载体,同时也是OpenVSwitch的载体,在本发明中用于定义流表规则限制到云主机的流量。