**Openstack的网络**

在理解network的配置之前你可以先规划好你的openstack的compute网络拓扑

networking options

    在compute中，用户在项目中组织他们云中的资源，一个compute中的项目包含一些用户创建的vm实例，对于每个vm，compute分配给vm一个私有ip地址，目前，compute只支持linux bridge模式的网络，让虚拟机通过物理网卡接口连接外面的网络。

    网络控制器提供虚拟网络，确保compute servers和公共网络可以相互作用。

    目前，compute支持三种类型的网络：

          Flat Network Manager

          Flat DHCP Network Manager

          VLAN Network Manager

    三种网络可以共存于一个云系统中...

    compute 控制虚拟机实例上面fixed ip和floating ip的差别，fixed ip是在实例创建时分配的ip，直到虚拟机terminated时也不会变化，而floating ip是动态分配给虚拟机实例的，一个floating ip可以取消或者分配给其他虚拟机实例在任何时间，用户可以给他们的项目存储floating ip

    Flat mode，网络管理员指定一个子网，vm实例获取的ip就来自此子网，并把它注入启动的镜像中，每个实例都会收到一个在可用的ip地址池中的fixed ip，网络管理员必须设置linux 网桥模式（一般命名为br100)，它同时控制主机网络和云中实例的网络，所有的实例都连接在同一个网桥上面。

    Flat DHCP Mode，你启动一个dhcp服务，在指定的子网中选择ip分发给vm实例，就像Flat mode一样，所有的实例都连接在同一个网桥上面，dhcp服务运行用来配置实例，在这种模式下，compute试图桥接一个以太网设备(默认是eth0)，还会运行一个dnsmasq作为dhcpserver监听网桥，实例通过dhcpdiscover接受他们的fixed ip

    在两种flat mode下，网络节点不作为网关。

    VLAN network mode，是默认的网络模式，在这种模式下，compute对每一个项目(project)创建vlan和网桥，在多节点安装中，vlan mode需要交换机支持802.1q标签，每个项目获取一个私网地址段落从inside vlan，为了使用户可以访问他们项目中的实例，一个指定的vpn实例(cloudpipe)需要被创建，......

    注意：在默认的compute设置中，一旦虚拟机实例被破坏后，会花一些时间使销毁实例的ip变为可用的fixed ip。当force\_dhcp\_release=true配置选项被设置的时候，会引起compute服务发送一个dhcp release包当destroy一个虚拟机实例的时候，它会使分配给实例的ip立刻释放掉。

    在compute 节点上配置networking，主要有以下几步：

    1 在/etc/nova/nova.conf中设置network-manager选项

    2 使用nova-manage network create label CIDR n n创建子网

    3 配置网桥

      compute默认使用vlan mode，可以在nova.conf中为你的虚拟机实例选择网络模式，有以下三个选项：

      network\_manager=nova.network.manager.FlatManager

      network\_manager=nova.network.manager.FlatDHCPManager

      network\_manager=nova.network.manager.VlanManager

configuring flat networking

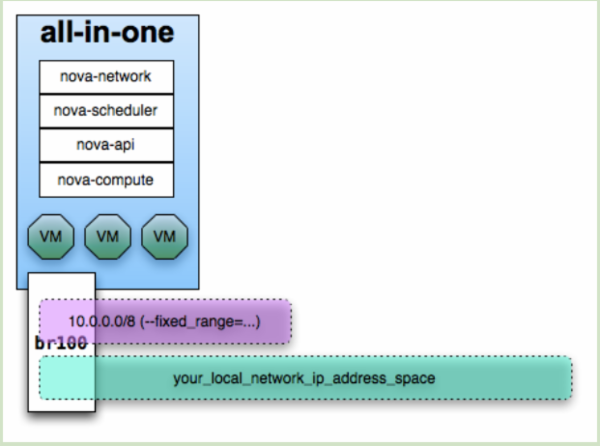
    flat network使用以太网适配器做桥接，允许网络流量通过各个节点，这个设置可以使用一个物理机或者多个物理机上的一个以太网适配器，不需要交换机设置标签，这是一般的安装步骤，当你选择了flat network，nova 不会管理networking，所以ip地址注入虚拟机实例是通过文件系统，数据的转发需要在网关上手动设置，配置flat network，确保在Nova.conf中：network\_manager=nova.network.manager.FlatManager，当配置了flat network，将不会开启flat\_injection，在引导时vm将会拒绝接受ip信息。

libvirt flat networking

    compute默认的网桥设备名称为br100，它是在nova 数据库中定义的，所以你可以修改数据库来修改网桥名称，在建立flat network网络，不论是flat还是flatDHCP，主机上的nova-network负责转发私有网络的流量通过配置nova.conf中的--fixed\_range= 和--flat\_network\_bridge，the default gateway for the virtual machines is set to the host which is running nova-network.

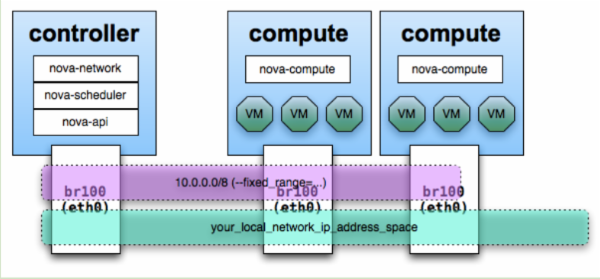
For an all-in-one development setup, this diagram represents the network setup.

Flat network, all-in-one server installation



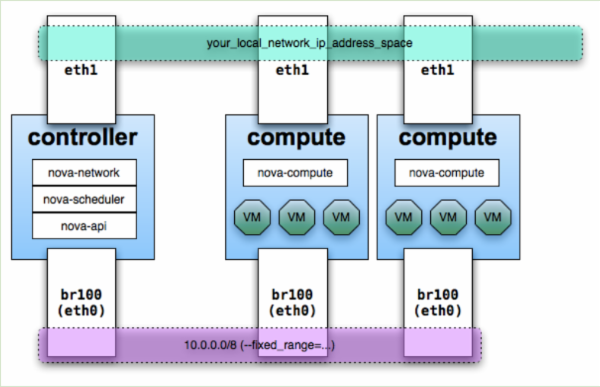
For multiple compute nodes with a single network adapter, which you can use for smoke testing or a proof of concept, this diagram represents the network setup

Flat network, single interface, multiple servers



For multiple compute nodes with multiple network adapters, this diagram represents the network setup. You may want to use this setup for separate admin and data traffic.

Flat network, multiple interfaces, multiple servers

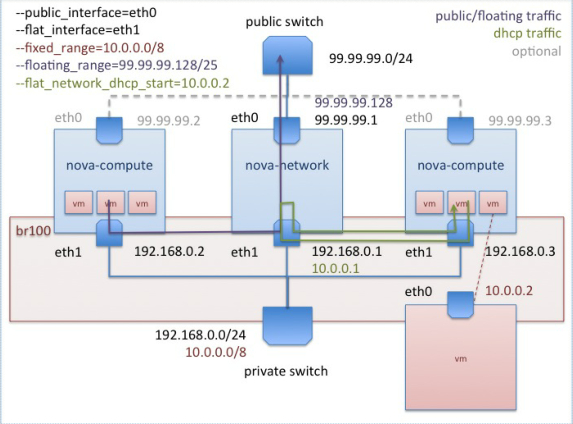


Configuring Flat DHCP Networking

    在flat dhcp中，主机运行Nova-network作为虚拟机的gateway，你可以在一个cluster中运行一个nova-network，设置network\_host在nova.conf中(在nova-compute)告诉那个主机运行了nova-network。nova-network服务会跟踪租期和释放ip在数据库中，所以一个实例stop的时候它是知道的，最后他设置iptables规则允许vm实例和外面的世界进行通讯，compute主机在flatdhcp模式下负责启动一个匹配的网桥，并且桥接vm实例的tap设备到同一个相同的网络，compute不需要vm 网络的ip，因为桥接使得vm和本机的网络在一个逻辑网络里面，当vm引导时，vm发出dhcp包，而在主机上的dhcp服务回复它分配的ip。flatdhcp不创建vlan，它创建网桥，这个网桥在单个主机上工作的很好，但是如果有多个主机，traffic needs a way to get out of the bridge onto a physical interface.

Libvirt Flat DHCP Networking

Flat DHCP network, multiple interfaces, multiple servers with libvirt driver



   在设置--flat\_interface的时候要小心，如果你指定的端口已经配置了ip，那么他就会被破坏掉，你也不能使用这个端口连接ssh，在flat dhcp模式，设置的--network-size的大小应该是处于fixed range之间，如果你定义了一个a/12的cidr，这样他就有2^20个ip(1048576)，这样当你创建网络时会花费很长的时间，如果你有一个未使用的端口，没有配置ip，有感简单的告诉flat dhcp在指定的端口进行桥接在你的配置文件中flat\_interface=ethx，主机网络会自动的给这个桥接增加网关ip，你也可以不设置flat\_interface，手动设置br100。

enabling ping and ssh on vms

你可以使用nova secgroup-add-rule 增加规则，使你可以访问vm，这个命令需要使用root权限。

nova secgroup-add-rule default icmp -1 -1 -s 0.0.0.0/0

nova secgroup-add-rule default tcp 22 22 -s 0.0.0.0/0

如果增加规则后你还是不能和vm通讯，查看一下dnsmasq进程是否在运行，如果你开启了一个实例，查看是否有两个dnsmasq进程在运行，如果不是，则killall dnsmasq;service nova-network restart

configuring public(floating) ip address

private and public ip address

    每个虚拟机都会自动的分配一个私网地址，你可以随意的分配公网ip给虚拟机实例。openstack使用“floating ip”指定一个公网ip到一个运行着的虚拟机实例上面，openstack使用NAT分配floating ip到虚拟机实例上。如果你想使用这种特性，你必须在nova.conf特别指定那个接口绑定公网ip，public\_interface=ethx，重启nova-network服务。

创建floating ip

    nova维护一个可用的floating ip列表，可以使用nova-manage floating create命令创建这个列表：

    nova-manage floating create --ip\_range=68.99.26.170/31

    nova-manage floating list  显示地址池中的ip

    nova-manage floating create [cidr] 创建floating ip，单个或者一个子网

    nova-manage floating delete [cidr]  删除floating ip

给实例绑定floating ip

    nova floating-ip-create 在floating ip池中分配一个floating ip

    nova add-floating-ip 把分配出来的floating ip绑定到运行着的虚拟机上面

    如果虚拟机长时间不需要公网地址，则可以溢出公网地址在实例上，然后回收地址

    nova remove-floating-ip SERVER IP

    nova floating-ip-delete IP

自动分配绑定ip公网ip

    当你启动一个虚拟机实例的时候nova-network服务可以被配制成自动的分配和分发一个floating ip到虚拟机，配置nova.conf加入如下配置：

    auto\_assign\_floating\_ip=true

    注意：如果你开启了这个选项，并且所有的floating ip已经分配完毕，会导致你在nova boot的时候启动失败。

    使用ip addr可以检查到你申请的floating ip已经绑定到公网上面了

移除一个项目中的网络

    在一个网络已经分配给一个项目的情况下，你不能删除这个网络，你必须先使网络和项目分离，使用如下命令：

    nova-manage project scrub projectname

在你的虚拟机实例中配置多个网卡

    multi-nic特性允许你在你的实例中配置多个网卡，可用于如下方面：

    SSL Configurations (VIPs)

    Services failover/ HA

    Bandwidth Allocation

    Administrative/ Public access to your instances