**Morning：**

1. 集群简介

What‘s集群：

-很多服务器集中起来，提供同一种服务，客户端看来只有一个服务器。

-核心技术：任务调度

集群目的：

-提高性能（计算力） ---> 高性能计算集群（HPC）

-降低成本（取代超级计算机）

-可扩展性（随意增加节点）

-负载均衡 ---> 负载均衡集群（LB）

-可靠性（避免单点失效） ---> 高可用集群（HA）

1. LVS概述

LVS基于内核，性能优于其他集群软件。

**-LVS集群组成**

前端（调度器）-- 中间（服务器集群）-- 底端（数据存储）

关于CIP、VIP、DIP、RIP：

--- Real Server1（RIP1）

Client --- （VIP）Director Server（DIP）

（CIP） --- Real Server2（RIP2）



**-LVS工作模式**

1. NAT模式

-原理： 调度器接收请求后，源IP不变 目标IP->RIP

Web收到请求后，原路返回。

-调度器必须开启路由转发功能；后端服务器必须添加网关。

-当并发量大，调度服务器会成为瓶颈(请求很小，回包很大)

-必须保证所有后端服务器的默认网关一致(同一广播域最大只能200台)

1. TUN模式

-原理：当调度器与后端服务器不在同一区域，通过隧道相连

-比较少用

3）DR模式

-原理：调度器修改数据链路层的dMAC，在数据链路层把数据帧转发给后端服务器，后端服务器直接返回给用户。



1. FULL-NAT模式

原理：调度器接收数据包后，源IP、目标IP同时改变

拓展架构： LVS(full-nat)+OSPF实现负载均衡集群及LVS集群

DPDK+LVS(full-nat)提高LVS性能

**-LVS调度算法**

-轮询：将客户端请求平均分发到Real Server

-加权轮询：根据Real Server的预设权重进行轮询调度

-最少连接：选择连接数最少的服务器

-加权最少连接：根据Real Server的预设权重，选择连接数最少的服务器

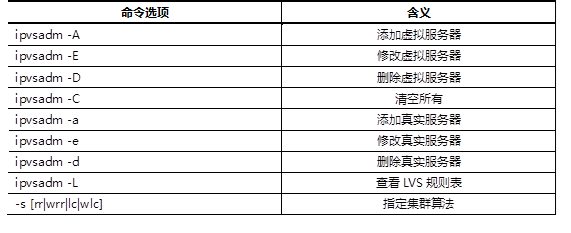
-源地址散列：Source Hashing（相当于IP hash）

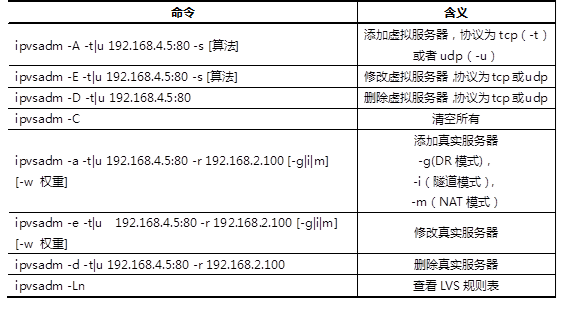
... ...

1. ipvsadm

**-ipvsadm命令列表**

[root@proxy ~]# man ipvsadm





**-使用ipvsadm命令（临时直接生效）**

1）安装ipvsadm，创建LVS虚拟集群服务器

[root@proxy ~]# yum -y install ipvsadm #管理内核的工具

[root@proxy ~]# ipvsadm -A -t 192.168.4.5:80 -s wrr

#-A创建集群 -t协议 -s算法

[root@proxy ~]# ipvsadm -Ln

#-Ln查看LVS规则表

2）为集群添加real server

[root@proxy ~]# ipvsadm -a -t 192.168.4.5:80 -r 192.168.2.100 -m -w 1

#-a添加Real Server -r真实服务器IP -m NAT模式 -w权重

3）修改集群服务器设置

[root@proxy ~]# ipvsadm -E -t 192.168.4.5:80 -s rr

4）修改Real Server设置

[root@proxy ~]# ipvsadm -e -t 192.168.4.5:80 -r 192.168.2.100 -g

1. 删除集群服务器

[root@proxy ~]# ipvsadm -D -t 192.168.4.5:80

1. 删除Real Server

[root@proxy ~]# ipvsadm -d -t 192.168.4.5:80 -r 192.168.4.100

7）清空所有规则

[root@proxy ~]# ipvsadm -C

8）永久保存所有规则

[root@proxy ~]# ipvsadm-save -n > /etc/sysconfig/ipvsadm

1. 重启|开机自启ipvadm

[root@proxy ~]# systemctl restart|enable ipvsadm

1. LVS-NAT集群

**-实验拓扑**



Tips：web1、web2需要设置网关为192.168.2.5

LVS调度器需要开启路由转发功能

web服务器的RIP与客户机**不可以为同一个网段**

**步骤1：配置基础环境**

虚拟机Web1、Web2搭建Web服务器

**步骤2：部署LVS-NAT模式调度器**

1）调度器开启路由转发功能

[root@proxy ~]# echo 1 > /proc/sys/net/ipv4/ip\_forward

#临时开启路由转发

[root@proxy ~]# echo "net.ipv4.ip\_forward = 1" >> /etc/sysctl.conf

#修改内核参数，设置永久路由转发

2）创建集群服务器+真实服务器

[root@proxy ~]# ipvsadm -A -t 192.168.4.5:80 -s wrr

[root@proxy ~]# ipvsadm -a -t 192.168.4.5:80 -r 192.168.2.100 -m

[root@proxy ~]# ipvsadm -a -t 192.168.4.5:80 -r 192.168.2.200 -m

1. 检查规则，保存设置

[root@proxy ~]# ipvsadm -Ln

[root@proxy ~]# ipvsadm-save -n > /etc/sysconfig/ipvsadm

[root@proxy ~]# systemctl enable ipvsadm

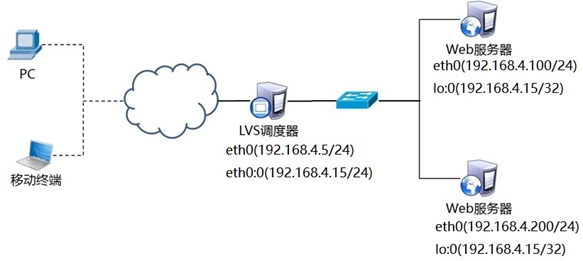
**步骤3：客户端验证**

[root@client ~]# curl 192.168.4.5

**Afternoon：**

1、LVS-DR集群

**-实验拓扑**



Tips：调度器eth0:0配VIP：192.168.4.15/24

Web服务器lo:0配VIP值，子网掩码/32（与任何主机都不同网段）

Web服务器必须可以与客户机不通过LVS调度器及进行通讯

**步骤1：配置网络环境**

1）设置proxy的VIP和DIP

[root@proxy ~]# cd /etc/sysconfig/network-scripts/

[root@proxy network-scripts]# cp ifcfg-eth0{,:0}

[root@proxy network-scripts]# vim ifcfg-eth0:0

TYPE=Ethernet

BOOTPROTO=static

NAME=eth0:0

DEVICE=eth0:0

ONBOOT=yes

IPADDR=192.168.4.15

PREFIX=24

#设置proxy代理服务器的VIP

[root@proxy network-scripts]# systemctl restart network

2）设置Web1的网络参数

[root@web1 ~]# nmcli connection .. eth0 .. 192.168.4.100/24

[root@web1 ~]# nmcli connection up eth0

#配置Web1的真实IP

[root@web1 ~]# cd /etc/sysconfig/network-scripts/

[root@web1 network-scripts]# cp ifcfg-lo{,:0}

[root@web1 network-scripts]# vim ifcfg-lo:0

DEVICE=lo:0

IPADDR=192.168.4.15

NETMASK=255.255.255.255

NETWORK=192.168.4.15

BROADCAST=192.168.4.15

ONBOOT=yes

NAME=lo:0

#配置lo:0的虚拟接口IP（与proxy的VIP一样，子网/32）

[root@web1 ~]# vim /etc/sysctl.conf

net.ipv4.conf.all.arp\_ignore = 1

net.ipv4.conf.lo.arp\_ignore = 1

net.ipv4.conf.lo.arp\_announce = 2

net.ipv4.conf.all.arp\_announce = 2

#设置内核参数，本机忽略询问192.168.4.15的ARP广播，不做回应

#本机不向外宣称自己的lo回环地址是192.168.4.15

#all指eth\*所有网卡，lo指回环

[root@web1 ~]# sysctl -p #将设置的参数写入到内核

[root@web2 ~]# systemctl restart network

3）设置Web2的网络参数

#配置Web2的真实IP：192.168.4.200/24

#配置Web2的lo:0虚拟接口IP：192.168.4.15/32

#设置内核参数，sysctl -p配置生效

#重启network，关闭防火墙、SElinux

**步骤2：配置后端Web服务器**

Web1：echo "192.168.4.100" > /var/www/html/index.html

Web2：echo "192.168.4.200" > /var/www/html/index.html

**步骤3：proxy部署LVS-DR模式调度器**

[root@proxy ~]#ipvsadm -A -t 192.168.4.15:80 -s wrr

[root@proxy ~]#ipvsadm -a -t 192.168.4.15:80 -r 192.168.4.100 -g -w 1

[root@proxy ~]#ipvsadm -a -t 192.168.4.15:80 -r 192.168.4.200 -g -w 1

[root@proxy ~]# ipvsadm-save -n > /etc/sysconfig/ipvsadm

**步骤4：客户端测试**

[root@client ~]# curl 192.168.4.5

**步骤5：LVS的健康检查**

[root@proxy ~]# cat /root/lvs-health.sh

#!/bin/bash

VIP="192.168.4.15"

RIP=("192.168.4.100" "192.168.4.200")

while :

do

for rip in ${RIP[@]}

do

curl $rip &> /dev/null

flag\_health=$?

ipvsadm -Ln | grep -q $rip

if [ $flag\_health -eq 0 ];then

[ $flag\_rip -eq 0 ] || ipvsadm -a -t ${VIP}:80 -r $rip -g

else

[ $flag\_rip -eq 0 ] && ipvsadm -d -t ${VIP}:80 -r $rip

fi

done

sleep 3

done

[root@proxy ~]# echo '/root/lvs-health.sh &' >> /etc/rc.local

#开机自动后台启动

**【拓展】使用ARP防火墙防止ARP冲突**

