[Top](http://tts.tmooc.cn/ttsPage/LINUX/NSDTN201904/CLUSTER/DAY01/CASE/01/index.html" \l "page_top_case)

# NSD CLUSTER DAY01

1. [案例1：ipvsadm命令用法](http://tts.tmooc.cn/ttsPage/LINUX/NSDTN201904/CLUSTER/DAY01/CASE/01/index.html" \l "case1)
2. [案例2：部署LVS-NAT集群](http://tts.tmooc.cn/ttsPage/LINUX/NSDTN201904/CLUSTER/DAY01/CASE/01/index.html" \l "case2)
3. [案例3：部署LVS-DR集群](http://tts.tmooc.cn/ttsPage/LINUX/NSDTN201904/CLUSTER/DAY01/CASE/01/index.html" \l "case3)

## 1 案例1：ipvsadm命令用法

### 1.1 问题

准备一台Linux服务器，安装ipvsadm软件包，练习使用ipvsadm命令，实现如下功能：

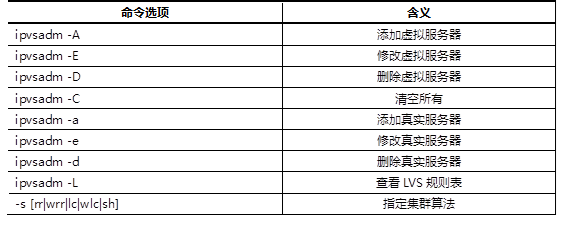
* 使用命令添加基于TCP一些的集群服务
* 在集群中添加若干台后端真实服务器
* 实现同一客户端访问，调度器分配固定服务器
* 会使用ipvsadm实现规则的增、删、改
* 保存ipvsadm规则

### 1.2 方案

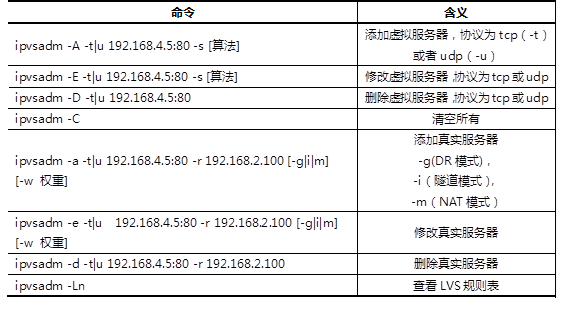
安装ipvsadm软件包，关于ipvsadm的用法可以参考man ipvsadm资料。

常用ipvsadm命令语法格式如表-1及表-2所示。

表－1 ipvsadm命令选项



表－2 ipvsadm语法案例



### 1.3 步骤

实现此案例需要按照如下步骤进行。

步骤一：使用命令增、删、改LVS集群规则

1）创建LVS虚拟集群服务器（算法为加权轮询：wrr）

1. [root@proxy ~]# yum -y install ipvsadm
2. [root@proxy ~]# ipvsadm -A -t 192.168.4.5:80 -s wrr
3. [root@proxy ~]# ipvsadm -Ln
4. IP Virtual Server version 1.2.1 (size=4096)
5. Prot LocalAddress:Port Scheduler Flags
6. -> RemoteAddress:Port Forward Weight ActiveConn InActConn
7. TCP 192.168.4.5:80 wrr

2）为集群添加若干real server

1. [root@proxy ~]# ipvsadm -a -t 192.168.4.5:80 -r 192.168.2.100
2. [root@proxy ~]# ipvsadm -Ln
3. IP Virtual Server version 1.2.1 (size=4096)
4. Prot LocalAddress:Port Scheduler Flags
5. -> RemoteAddress:Port Forward Weight ActiveConn InActConn
6. TCP 192.168.4.5:80 wrr
7. -> 192.168.2.100:80 router 1 0 0
8. [root@proxy ~]# ipvsadm -a -t 192.168.4.5:80 -r 192.168.2.200 -m -w 2
9. [root@proxy ~]# ipvsadm -a -t 192.168.4.5:80 -r 192.168.2.201 -m -w 3
10. [root@proxy ~]# ipvsadm -a -t 192.168.4.5:80 -r 192.168.2.202 -m -w 4

3）修改集群服务器设置(修改调度器算法，将加权轮询修改为轮询)

1. [root@proxy ~]# ipvsadm -E -t 192.168.4.5:80 -s rr
2. [root@proxy ~]# ipvsadm -Ln
3. IP Virtual Server version 1.2.1 (size=4096)
4. Prot LocalAddress:Port Scheduler Flags
5. -> RemoteAddress:Port Forward Weight ActiveConn InActConn
6. TCP 192.168.4.5:80 rr
7. -> 192.168.2.100:80 router 1 0 0
8. -> 192.168.2.200:80 masq 2 0 0
9. -> 192.168.2.201:80 masq 2 0 0
10. -> 192.168.2.202:80 masq 1 0 0

4）修改read server（使用-g选项，将模式改为DR模式）

1. [root@proxy ~]# ipvsadm -e -t 192.168.4.5:80 -r 192.168.2.202 -g

5）查看LVS状态

1. [root@proxy ~]# ipvsadm -Ln

6）创建另一个集群（算法为最少连接算法；使用-m选项，设置工作模式为NAT模式）

1. [root@proxy ~]# ipvsadm -A -t 192.168.4.5:3306 -s lc
2. [root@proxy ~]# ipvsadm -a -t 192.168.4.5:3306 -r 192.168.2.100 -m
3. [root@proxy ~]# ipvsadm -a -t 192.168.4.5:3306 -r 192.168.2.200 -m

7）永久保存所有规则

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

8）清空所有规则

1. [root@proxy ~]# ipvsadm -C

## 2 案例2：部署LVS-NAT集群

### 2.1 问题

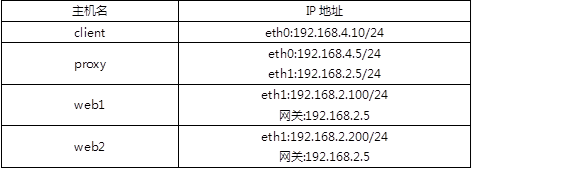
使用LVS实现NAT模式的集群调度服务器，为用户提供Web服务：

* 集群对外公网IP地址为192.168.4.5
* 调度器内网IP地址为192.168.2.5
* 真实Web服务器地址分别为192.168.2.100、192.168.2.200
* 使用加权轮询调度算法，真实服务器权重分别为1和2

### 2.2 方案

实验拓扑结构主机配置细节如表-3所示。

表-3



使用4台虚拟机，1台作为Director调度器、2台作为Real Server、1台客户端，拓扑结构如图-1所示，注意：web1和web2必须配置网关地址。



图-1

### 2.3 步骤

实现此案例需要按照如下步骤进行。

步骤一：配置基础环境

1）设置Web服务器（以web1为例）

1. [root@web1 ~]# yum -y install httpd
2. [root@web1 ~]# echo "192.168.2.100" > /var/www/html/index.html

2）启动Web服务器软件

1. [root@web1 ~]# systemctl restart httpd

常见问题：如果httpd服务启动启动的比较慢？

解决方法：可以修改/etc/httpd/conf/httpd.conf文件，

将ServerName www.example.com:80这行的#注释符删除即可。

步骤二：部署LVS-NAT模式调度器

1)确认调度器的路由转发功能(如果已经开启，可以忽略)

1. [root@proxy ~]# echo 1 > /proc/sys/net/ipv4/ip\_forward
2. [root@proxy ~]# cat /proc/sys/net/ipv4/ip\_forward
3. 1
4. [root@proxy ~]# echo "net.ipv4.ip\_forward = 1" >> /etc/sysctl.conf
5. #修改配置文件，设置永久规则

2）创建集群服务器

1. [root@proxy ~]# yum -y install ipvsadm
2. [root@proxy ~]# ipvsadm -A -t 192.168.4.5:80 -s wrr

3）添加真实服务器

1. [root@proxy ~]# ipvsadm -a -t 192.168.4.5:80 -r 192.168.2.100 -w 1 -m
2. [root@proxy ~]# ipvsadm -a -t 192.168.4.5:80 -r 192.168.2.200 -w 1 -m

4）查看规则列表，并保存规则

1. [root@proxy ~]# ipvsadm -Ln
2. [root@proxy ~]# ipvsadm-save -n > /etc/sysconfig/ipvsadm

步骤三：客户端测试

客户端使用curl命令反复连接http://192.168.4.5，查看访问的页面是否会轮询到不同的后端真实服务器。

## 3 案例3：部署LVS-DR集群

### 3.1 问题

使用LVS实现DR模式的集群调度服务器，为用户提供Web服务：

* 客户端IP地址为192.168.4.10
* LVS调度器VIP地址为192.168.4.15
* LVS调度器DIP地址设置为192.168.4.5
* 真实Web服务器地址分别为192.168.4.100、192.168.4.200
* 使用加权轮询调度算法，web1的权重为1，web2的权重为2

说明：

CIP是客户端的IP地址；

VIP是对客户端提供服务的IP地址；

RIP是后端服务器的真实IP地址；

DIP是调度器与后端服务器通信的IP地址（VIP必须配置在虚拟接口）。

### 3.2 方案

使用4台虚拟机，1台作为客户端、1台作为Director调度器、2台作为Real Server，拓扑结构如图-2所示。实验拓扑结构主机配置细节如表-4所示。

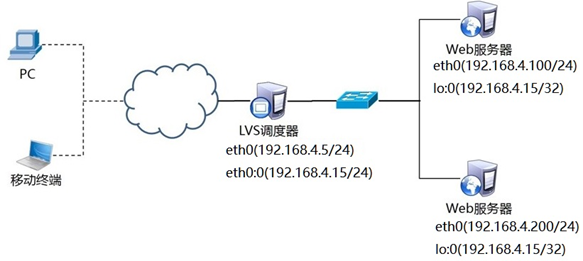
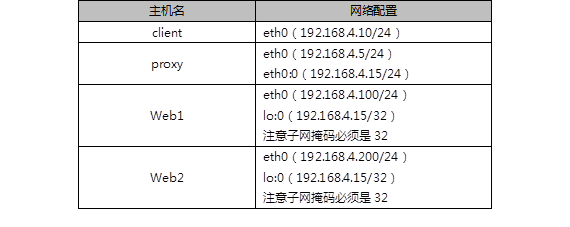


图-2

表-4



### 3.3 步骤

实现此案例需要按照如下步骤进行。

说明：

CIP是客户端的IP地址；

VIP是对客户端提供服务的IP地址；

RIP是后端服务器的真实IP地址；

DIP是调度器与后端服务器通信的IP地址（VIP必须配置在虚拟接口）。

步骤一：配置实验网络环境

1）设置Proxy服务器的VIP和DIP

注意：为了防止冲突，VIP必须要配置在网卡的虚拟接口！！！

1. [root@proxy ~]# cd /etc/sysconfig/network-scripts/
2. [root@proxy ~]# cp ifcfg-eth0{,:0}
3. [root@proxy ~]# vim ifcfg-eth0:0
4. TYPE=Ethernet
5. #网卡类型为：以太网卡
6. BOOTPROTO=none
7. #none手动配置IP，或者dhcp自动配置IP
8. NAME=eth0:0
9. #网卡名称
10. DEVICE=eth0:0
11. #设备名称
12. ONBOOT=yes
13. #开机时是否自动激活该网卡
14. IPADDR=192.168.4.15
15. #IP地址
16. PREFIX=24
17. #子网掩码
18. [root@proxy ~]# systemctl restart network
19. [root@proxy ~]# ifconfig

常见问题：RHEL7和Centos7系统中有两个管理网络的服务，有可能冲突？

解决方法：关闭NetworkManager服务后重启network即可。

2）设置Web1服务器网络参数

1. [root@web1 ~]# nmcli connection modify eth0 ipv4.method manual \
2. ipv4.addresses 192.168.4.100/24 connection.autoconnect yes
3. [root@web1 ~]# nmcli connection up eth0

接下来给web1配置VIP地址。

注意：这里的子网掩码必须是32（也就是全255），网络地址与IP地址一样，广播地址与IP地址也一样。

1. [root@web1 ~]# cd /etc/sysconfig/network-scripts/
2. [root@web1 ~]# cp ifcfg-lo{,:0}
3. [root@web1 ~]# vim ifcfg-lo:0
4. DEVICE=lo:0
5. IPADDR=192.168.4.15
6. NETMASK=255.255.255.255
7. NETWORK=192.168.4.15
8. BROADCAST=192.168.4.15
9. ONBOOT=yes
10. NAME=lo:0

防止地址冲突的问题：

这里因为web1也配置与调度器一样的VIP地址，默认肯定会出现地址冲突；

sysctl.conf文件写入这下面四行的主要目的就是访问192.168.4.15的数据包，只有调度器会响应，其他主机都不做任何响应，这样防止地址冲突的问题。

1. [root@web1 ~]# vim /etc/sysctl.conf
2. #手动写入如下4行内容
3. net.ipv4.conf.all.arp\_ignore = 1
4. net.ipv4.conf.lo.arp\_ignore = 1
5. net.ipv4.conf.lo.arp\_announce = 2
6. net.ipv4.conf.all.arp\_announce = 2
7. #当有arp广播问谁是192.168.4.15时，本机忽略该ARP广播，不做任何回应
8. #本机不要向外宣告自己的lo回环地址是192.168.4.15
9. [root@web1 ~]# sysctl -p

重启网络服务，设置防火墙与SELinux

1. [root@web1 ~]# systemctl restart network
2. [root@web1 ~]# ifconfig

常见错误：如果重启网络后未正确配置lo:0，有可能是NetworkManager和network服务有冲突，关闭NetworkManager后重启network即可。（非必须的操作）

1. [root@web1 ~]# systemctl stop NetworkManager
2. [root@web1 ~]# systemctl restart network

3）设置Web2服务器网络参数

1. [root@web2 ~]# nmcli connection modify eth0 ipv4.method manual \
2. ipv4.addresses 192.168.4.200/24 connection.autoconnect yes
3. [root@web2 ~]# nmcli connection up eth0

接下来给web2配置VIP地址

注意：这里的子网掩码必须是32（也就是全255），网络地址与IP地址一样，广播地址与IP地址也一样。

1. [root@web2 ~]# cd /etc/sysconfig/network-scripts/
2. [root@web2 ~]# cp ifcfg-lo{,:0}
3. [root@web2 ~]# vim ifcfg-lo:0
4. DEVICE=lo:0
5. IPADDR=192.168.4.15
6. NETMASK=255.255.255.255
7. NETWORK=192.168.4.15
8. BROADCAST=192.168.4.15
9. ONBOOT=yes
10. NAME=lo:0

防止地址冲突的问题：

这里因为web1也配置与调度器一样的VIP地址，默认肯定会出现地址冲突；

sysctl.conf文件写入这下面四行的主要目的就是访问192.168.4.15的数据包，只有调度器会响应，其他主机都不做任何响应，这样防止地址冲突的问题。

1. [root@web2 ~]# vim /etc/sysctl.conf
2. #手动写入如下4行内容
3. net.ipv4.conf.all.arp\_ignore = 1
4. net.ipv4.conf.lo.arp\_ignore = 1
5. net.ipv4.conf.lo.arp\_announce = 2
6. net.ipv4.conf.all.arp\_announce = 2
7. #当有arp广播问谁是192.168.4.15时，本机忽略该ARP广播，不做任何回应
8. #本机不要向外宣告自己的lo回环地址是192.168.4.15
9. [root@web2 ~]# sysctl -p

重启网络服务，设置防火墙与SELinux

1. [root@web2 ~]# systemctl restart network
2. [root@web2 ~]# ifconfig

常见错误：如果重启网络后未正确配置lo:0，有可能是NetworkManager和network服务有冲突，关闭NetworkManager后重启network即可。（非必须的操作）

1. [root@web1 ~]# systemctl stop NetworkManager
2. [root@web1 ~]# systemctl restart network

步骤二：proxy调度器安装软件并部署LVS-DR模式调度器

1）安装软件（如果已经安装，此步骤可以忽略）

1. [root@proxy ~]# yum -y install ipvsadm

2）清理之前实验的规则，创建新的集群服务器规则

1. [root@proxy ~]# ipvsadm -C #清空所有规则
2. [root@proxy ~]# ipvsadm -A -t 192.168.4.15:80 -s wrr

3）添加真实服务器(-g参数设置LVS工作模式为DR模式，-w设置权重)

1. [root@proxy ~]# ipvsadm -a -t 192.168.4.15:80 -r 192.168.4.100 -g -w 1
2. [root@proxy ~]# ipvsadm -a -t 192.168.4.15:80 -r 192.168.4.200 -g -w 1

4）查看规则列表，并保存规则

1. [root@proxy ~]# ipvsadm -Ln
2. TCP 192.168.4.15:80 wrr
3. -> 192.168.4.100:80 Route 1 0 0
4. -> 192.168.4.200:80 Route 2 0 0

步骤三：客户端测试

客户端使用curl命令反复连接http://192.168.4.15，查看访问的页面是否会轮询到不同的后端真实服务器。

扩展知识：默认LVS不带健康检查功能，需要自己手动编写动态检测脚本，实现该功能：(参考脚本如下，仅供参考)

1. [root@proxy ~]# vim check.sh
2. #!/bin/bash
3. VIP=192.168.4.15:80
4. RIP1=192.168.4.100
5. RIP2=192.168.4.200
6. while :
7. do
8. for IP in $RIP1 $RIP2
9. do
10. curl -s http://$IP &>/dev/vnull
11. if [ $? -eq 0 ];then
12. ipvsadm -Ln |grep -q $IP || ipvsadm -a -t $VIP -r $IP
13. else
14. ipvsadm -Ln |grep -q $IP && ipvsadm -d -t $VIP -r $IP
15. fi
16. done
17. sleep 1
18. done