IPVSADM Befehls Übersichts Seite

Das Kommando hat 2 grundlegende Formate der Ausführung:

ipvsadm Kommando[Protokoll] Service−Adresse
[Scheduling−Methode] [Persistenz Optionen]

ipvsadm Kommando [Protokoll] Service−Adresse
Server−Adresse [Packet−Weiterleitungs−Methode]
[Gewichtungs−Optionen]

Das erste Format manipuliert einen Virtual Service, und den Algorithmus in wie fern Service Anfragen zu einem Real Server zugewiesen werden. Optional kann ein persistenter Timeout mit Netzwerk Maske für die Granularität eines Persistenten Service zugewiesen werden. Das zweite Format manipuliert einen Real Server welcher mit einem existierenden virtuellen Service verbunden worden ist. Wenn ein Real Server spezifiziert wird, kann die Packet−Weiterleitungs− Methode und die Gewichtung von den Real Servern relativ zu anderen Real Servern für den virtuellen Service angegeben werden. Anderenfalls werden die Default Werte benutzt.

KOMMANDOS

ipvsadm erkennt untenstehende Kommandos. Kommandos in **Grossbuchstaben** bedeuten virtuelle Services. Kleingeschriebene Kommandos bedeuten Real Server welche mit einem Virtuellen Service assoziiert worden sind.

−A, −−add−service

−E, −−edit−service
Editieren eines Virtual Services.

−D, −−delete−service
Löschen eines virtuellen Services inclusive aller assoziierten Real Server.

−C, −−clear
Auflösen/Löschen der Virtual Server Tabelle.

−R, −−restore
Restaurieren der Linux Virtual Server Regeln von stdin. Jede Zeile von stdin wird wie ein separater Aufruf von ipvsadm abgehandelt. Zeilen welche von stdin gelsen werden, können optional mit "ipvsadm" beginnen.

−S, −−save
Dumpen der Linux Virtual Server regeln nach stdout zu einem Format welches von −R −−Restore gelesen werden kann.

IPVSADM Befehls Übersichts Seite

−a, −−add−Server
Einen Real Server zu einem Virtuellen Service hinzufügen.

−e, −−edit−Server
Editieren eines Real Servers in einem Virtuellen Service.

−d, −−delete−Server
Entfernen eines Real Servers von einem Virtuellen Service.

−L, −l, −−list
Auflisten der Virtual Server Tabelle, wenn kein Argument angegeben wurde. Wenn eine Service Adresse angegeben wurde, wird nur dieser Dienst angezeigt. Wenn die −c Option angegeben worden ist, wird die Verbindungs Tabelle angezeigt.

−Z, −−zero
Zurücksetzen des Packet,Byte und Raten Zählers in einem Service, oder allen Services.

−−set tcp tcpfin udp
Ändern der Timeout Werte benutzt für IPVS Verbindungen. Das Komando nimmt immer 3 Parameter, welche die Timeout Werte(in Sekunden) für TCP Sessions, TCP Sessions nach Empfang des FIN Packets, und respektive UDP Packete. Ein Timeout Wert von 0 bedeutet, das der aktuelle Timeout Wert des korrespondierenden Eintrags erhalten bleibt.

−−start−daemon state
Starten des Verbindungs−Synchronisations−Daemons. Er kann als Master oder Backup gestartet werde. Der Verbindungs−Synchronisations−Daemon ist im Linux Kernel implementiert. Der Master Deamon läuft auf dem primären Load Balancer und Multicastet Periodisch Änderungen der Verbindungen. Der Backup Daemon welcher auf dem Backup Load Balancer läuft empfängt Periodisch die Multicast−Änderungen der Verbindungen und kreiert korrespondierende Verbindungen. Gesetzt den Fall, das der primäre Load Balancer ausfällt, übernimmt ein Backup Load Balancer, die Zustands−Verbindungen von den meisten etablierten Verbindungen, so dass die meisten etablierten Verbindungen weiter den zugewiesenen Dienst benutzen können.

−−stop−daemon
Stopt den Verbindungs−Synchronizations−Daemon.

−h, −−help
Anzeige der Beschreibung des Kommando Syntax.

PARAMETERS

Die Kommandos unterhalb akzeptieren, oder benötigen keine oder mehrere der folgenden Parameter.

−t, −−tcp−service service−Addresse
Benutze den TCP Dienst. Die Service Adresse ist in der Form von Host[:Port]. Host kann eine gültige IP Adresse oder ein gültiger DNS Hostname sein. Der Port kann eine gültige Port Nummer oder ein Service Name eines Ports sein. Der Port kann auch ausgelassen werden, in dem Fall wird 0 als Portnummer eingetragen. Ein Port mit 0 als Adresse ist nur gültig, wenn der Dienst persistent wie mit der −pl −−persistent Option angegeben worden ist. In diesem Fall ist es ein Wild− Card Port, zu dem Verbindungen zu jedem Port zugelassen werden.

−u, −−udp−service service−Adresse
Benutze den UDP Dienst. Siehe −t|−−tcp−Dienst für die Beschreibung der Service−Adresse.

−f, −−fwmark−service Ganzzahl
Benutze eine Firewall Markierung, einen Ganzzahlwert größer als 0, um einen Virtuellen Service anzudeuten anstatt einer Adresse, eines Ports und eines Protokolls (UDP oder TCP). Das markieren von Packeten mit einer Firewall Markierung wird konfiguriert mit der −m|−−Markierungs Option von iptables(8). Sie kann benutzt werden um einen Virtuellen Service zu bauen der mit dem selben Real Server assoziiert wird um mehrere IP Adressen, Ports und Protokoll tripplets zu umhüllen.

Firewall markierte Virtuelle Services geben uns eine bequemere Methode verschiedene IP Adressen, Ports und Protokolle zu einem einzigen Virtuellen Service zu gruppieren. Das ist nützlich für eine einfachere Konfiguration, wenn eine große Anzahl von Virtuellen Diensten benötigt wird, und Gruppen− Persistents wichtiger ist als viele multiple Virtuelle Dienste.

IPVSADM Befehls Übersichts Seite

−s, −−scheduler scheduling−Methode
Scheduling−Methoden Algorithmus zur Zuweisung von TCP Verbindungen und UDP Datagrammen zu Real Servern. Scheduling Algorithmen sind implementiert als Kernel Module. Sechs Stück von ihnen werden mit dem Linux Virtual Server ausgeliefert:

rr − Robin Robin:
verteilt die Jobs gleichmäßig auf alle verfügbaren Real Server.

wrr − Gewichteter Round Robin:
Teilt Server ProPortional zu der Real Server Gewichtung zu. Server mit höherer Gewichtung bekommen neue Jobs zuerst, und bekommen mehr Jobs als Server mit niedriger Gewichtung. Server mit gleicher Gewichtung bekommen eine gleiche Verteilung von neuen Jobs.

lc − Least−Connection:
Weist mehr Jobs zu Real Servern mit weniger aktiven Jobs zu.

wlc − Weighted Least−Connection:
Weist mehr Jobs zu Servern mit weniger Jobs relativ zu der Real Server Gewichtung zu. Das ist die Default Einstellung

lblc − Locality−Based Least−Connection:
Weist Jobs welche in Richtung der selben IP Adresse gehen den selben Server zu, wenn der Server nicht mit Verbindungen überladen und verfügbar ist. Anderenfalls weist der Algorithmus Jobs Servern mit weniger Jobs zu, und behält diese Einstellung für zukünftige Zuweisungen bei.

lblcr − Locality−Based Least−Connection mit Replication:
Weist Jobs welche in Richtung der selben IP Adresse gehen, zu dem Node mit den wenigsten Verbindungen welche im Server Set für diese IP Adresse gelten. Wenn alle Nodes in dem Sever Set überladen sind,nimmt er einen Node mit weniger Jobs für das Ziel. Wenn der gesetzte Server in der spezifizierten Zeit nicht modifiziert worden ist, wird der am höchsten überladene Node vom Server Set entfernt, um hochgradige Replikation zu vermeiden.

IPVSADM Befehls Übersichts Seite

dh − Destination Hashing:
Weist Jobs zu Servern durch nachschlagen einer statisch zugewiesenen Hash Tabelle durch Ihre Ziel IP−Adresse zu.

sh − Source Hashing:
Weist Jobs zu Servern durch nachschlagen einer statisch zugewiesenen Hash Tabelle durch Ihre Quell IP−Adresse zu.

−p, −−persistent [timeout]
Spezifiziert, das ein virtueller Service persistent ist. Wenn diese Option spezifiziert ist, werden mehrfach Anfragen von einem Client zu dem selben Real Server weitergeleitet der für die erste Anfrage verantwortlich wahr. Optional kann der Timeout von persistenten Verbindungen in Sekunden angegeben werden. Anderenfalls wird der Default von 300 Sekunden benutzt. Diese Option sollte vielleicht in Verbindung mit Protokollen wie SSL oder FTP eingesetzt werden, wo es wichtig ist, das Clients konsistent Verbindung mit dem selben Real Server bekommen.

Anmerkung: Wenn ein virtueller Dienst FTP Verbindungen abhandeln soll, dann muss für den virtuellen Dienst **Persistenz** eingesetzt werden, wenn **Direct Routing** oder **Tunnelling** als weiterleitungs−mechanismus eingesetzt wird. Wenn Masquerading im Zusammenhang mit einem FTP Dienst eingesetzt wird, ist Persistenz nicht nötig, aber das ip vs ftp Kernel Modul muss dann benutzt werden. Dieses Modul kann möglicherweise Manuell in den Kernel mit insmod geladen werden.

−M, −−netmask netmask

Spezifiziert die Granulation mit dem bestimmte Clients für Persistente virtuelle Dienste gruppiert werden. Die Quell Adresse der Anfrage ist Maskiert mit der Teilnetzmaske um alle Clients von einem Netzwerk zu den selben Real Server zu dirigieren. Der Default Wert 255.255.255.255, bedeutet, die Persistente Granulation ist pro Client Host. Weniger spezifische Teilnetzmasken mögen benutzt werden, um Probleme mit Nicht Persistenten Cache Clustern auf der Client Seite zu lösen.

−r, −−Real−Server Server−Adresse
Real Server der eine assozierte Anfrage für einen Dienst zugewiesen wurde. Die Server Adresse ist die Host Adresse von einem Real Server, und kann eine Port Angabe beinhalten. Host kann eine gültige IP Adresse oder ein Hostname sein. Port kann eine gültige Port Nummer oder der Service Name eines Ports sein. Falls die Masquerading Methode benutzt wird, ist die Adresse gewöhnlicherweise eine in RFC 1918 spezifizierte private IP Adresse, und der Port kann von dem assoziierten Dienst verschieden sein. Mit der Tunnelling oder Direct Routing Methode muss der Port gleich zu der Dienst Adresse sein. Für normale Dienste wird der Port welcher in der Dienst Adresse spezifiziert wurde benutzt, wenn der Port nicht spezifisch angegeben wurde. Für fwmark Dienste kann der Port ausgelassen werden, in dem Fall ist der Ziel Port auf dem Real Server der Ziel Port der Anfrage welcher zu dem virtuellen Dienst gesendet wird.

[Packet−Weiterleitungs−Methode]

−g, −−gatewaying Benutze Gatewaying (Direct Routing). Das ist der Default.

−i, −−ipip Benutze ipip Verkapselung (Tunneling).

−m, −−masquerading Benutze Masquerading (Network Adress Translation, oder NAT).

Anmerkung: Egal welcher Packet−weiterleitungs− Mechanismus spezifiziert worden ist, Real Server für Adressen die Netzwerk Interfaces auf den lokalen Node haben werden die lokale weiterleitungs− Methode benutzen. die Packete für die Server werden dann den unteren Layer des lokalen Nodes passieren. Dies kann nicht durch ipvsadm spezifiziert werden, da diese Methode durch den Kernel gesetzt wird, wenn Server hinzugefügt oder modifiziert werden.

−n, −−numerisch
Numerische Ausgabe. IP Adressen und Port Nummern werden im Numerischen Format anstatt als Hostname beziehungsweise Dienste ausgegeben, was der Default ist.

IPVSADM Befehls Übersichts Seite

−w, −−weight Gewichtung
Die Gewichtung ist ein Ganzzahlwert die die Kapazität eines Servers relativ zu den anderen im Server Pool spezifiziert. Gültige Werte einer Gewichtung sind 0 bis 65535. Der Default ist 1. Server die keine neuen Verbindungen mehr annehmen sollen, werden mit einer Gewichtung von 0 spezifiziert. Ein derart ruhender Server wird keine neues Jobs mehr empfangen, aber die noch existenten Jobs in Ruhe für alle Scheduling Algorithmen welche mit dem Linux Virtual Server Projekt ausgeliefert werden abarbeiten. Einen ruhenden Server zu setzen kann nützlich sein, wenn der Server überladen ist, und aus dem Server Pool für allgemeine Maintenance entfernt werden soll.

−−mcast−interface interface
Spezifiziert das Multicast Interface durch das der Sync Master Daemon ausgehende Multicasts sendet, oder der Sync Backup Daemon horcht für die Multicasts.

−c, −−connection
Verbindungs Ausgabe. Das auflist Kommando mit dieser Option listet gegenwärtige IPVS Verbindungen.

−−timeout
Timeout Ausgabe. das auflist Kommando mit dieser Option listet die timeout Werte(in Sekunden) für TCP Sessions auf, TCP Sessions nach Empfang des FIN Packetes, und UDP Packete.

−−daemon
Daemon Zustands Ausgabe. Das auflist Kommando mit dieser Option zeigt den Daemon status und sein Multicast Interface an.

−−stats
Ausgabe von Statistik Informationen. Die Statistik Information der Dienste und ihrer Server wird dann angezeigt, wenn die Dienste gelistet sind.

−−rate Ausgabe der Daten Rate
Die rate Information (wie Verbindungen/Sekunde, Bytes/Sekunde und Packete/Sekunde) von Diensten und ihren Servern werden dann angezeigt, wenn die Dienste gelistet sind.

IPVSADM Befehls Übersichts Seite

BEISPIEL 1 − Einfache Virtuelle Dienste

Die folgenden Kommandos konfigurieren für einen Linux Director ankommende Anfragen zu Adressen nach Port 80 auf 207.175.44.110 gleichmäßig auf Port 80 an 5 Real Server zu verteilen. Die weiterleitungs Methode die dieses Beispiel benutzt ist NAT, mit jeden von den Real Servern maskiert durch den Linux Director.

```
ipvsadm −A −t 207.175.44.110:80 −s rr
ipvsadm −a −t 207.175.44.110:80 −r 192.168.10.1:80 −m
ipvsadm −a −t 207.175.44.110:80 −r 192.168.10.2:80 −m
ipvsadm −a −t 207.175.44.110:80 −r 192.168.10.3:80 −m
ipvsadm −a −t 207.175.44.110:80 −r 192.168.10.4:80 −m
ipvsadm −a −t 207.175.44.110:80 −r 192.168.10.5:80 −m
```

Alternativerweise kann dies auch durch ein einzelnes ipvsadm Kommando erzeugt werden.

```
echo "
−A −t 207.175.44.110:80 −s rr
−a −t 207.175.44.110:80 −r 192.168.10.1:80 −m
−a −t 207.175.44.110:80 −r 192.168.10.2:80 −m
−a −t 207.175.44.110:80 −r 192.168.10.3:80 −m
−a −t 207.175.44.110:80 −r 192.168.10.4:80 −m
−a −t 207.175.44.110:80 −r 192.168.10.5:80 −m
" | ipvsadm −R
```

Masquerading wird in diesem Beispiel als weiterleitungs Mechanismuss benutzt, in diesem Fall muss die Default Route von den Real Servern zu dem Linux Director gesetzt werden, welche benötigt wird, um Packete weiterleiten und Maskieren zu können. Das kann durch folgendes Kommandos erreicht werden:

```
echo "1" > /proc/sys/net/ipv4/ip forward
```

BEISPIEL 2 − Firewall−Markierte Virtuelle Dienste

Die folgenden Kommandos konfigurieren für einen Linux Director ankommende Anfrage−Adressen zu jedem Port auf 207.175.44.110 oder 207.175.44.111 gleichmäßig zu dem korrespondierend Port auf fünf Real Servern zu verteilen. Wie das vorhergehende Beispiel ist die weiterleitungs− Methode in diesem Beispiel NAT, mit jedem der Real Server maskiert durch den Linux Director.

```
ipvsadm −A −f 1  −s rr
ipvsadm −a −f 1 −r 192.168.10.1:0 −m
ipvsadm −a −f 1 −r 192.168.10.2:0 −m
ipvsadm −a −f 1 −r 192.168.10.3:0 −m
ipvsadm −a −f 1 −r 192.168.10.4:0 −m
ipvsadm −a −f 1 −r 192.168.10.5:0 −m
```

Masquerading wird in diesem Beispiel als weiterleitungs Mechanismus benutzt. Die Default Route von den Real Servern muss zu dem Linux Director gesetzt sein um Packete weiterleiten und maskieren zu können. Die Real Server sollten ausserdem so konfiguriert werden, das sie ankommende Packet−Adressen markieren zu jedem Port an 207.175.44.110 und 207.175.44.111 mit dem firewall−mark 1. Wenn FTP Verkehr von diesem Virtuellen Service abgehandelt werden sollen, ist das **ip vs ftp Kernel Modul** in den Kernel zu laden. Diese Operationen können durch folgende Kommandos erreicht werden:

```
echo "1" > /proc/sys/net/ipv4/ip forward
/sbin/modprobe iptables
/sbin/iptables  −A PREROUTING −t mangle −d 207.175.44.110/31 −j MARK −−set−mark 1
/sbin/modprobe ip vs ftp
```

ANMERKUNG:

Der Linux Virtual Server implementiert drei defensive Strategien gegen einige Typen von Denial of Service (DoS) Attacken. Der Linux Director kreiert einen Eintrag für jede Verbindung um den Zustand zu halten, und jeder Eintrag besetzt 128 Bytes effektiven Speichers. LVS's Verwundbarkeit zu einem DoS Angriff liegt in dem Potential die Nummer aller Einträge so schnell wie möglich zu erhöhen bis der Linux Director zuwenig Speicher hat.

Die drei defensiv Strategien gegen die Attacken sind: Zufallsmässig einige Einträge in der Tabelle zurückweisen. Zurückweisen von 1/rate Packeten bevor sie weitergeleitet werden. Und der Gebrauch von sicheren TCP zustands− verbindungs Tabellen mit kurzen timeouts. Diese Strategien werden durch sysctl Variablen und korrespondierend Einträge im /proc Dateisystem festgelegt:

/proc/sys/net/ipv4/vs/drop entry
/proc/sys/net/ipv4/vs/drop packet
/proc/sys/net/ipv4/vs/secure tcp

Gültige Einträge für jede Variable sind 0 bis 3. Der Default Wert ist 0, welches die entsprechende Verteidigungs− Strategie sperrt. 1 und 2 sind automatische Moden − wenn es nicht mehr genug Speicher gibt, wird die jeweilige Strategie automatisch aktiviert und die Variable automatisch auf 2 gesetzt, anderenfalls ist die Strategie gesperrt und die Variable auf 1 gesetzt. Ein Wert von 3 bezeichnet das die entsprechende Strategie immer aktiviert ist. Der vorhandene Hauptspeicher Schwellwert und sichere TCP timeouts können durch die sysctl Variablen und korespondierende Einträge im /proc Dateisystem getuned werden:

/proc/sys/net/ipv4/vs/amemthresh
/proc/sys/net/ipv4/vs/timeout *

DATEIEN

/proc/net/ip vs
/proc/net/ip vs app
/proc/net/ip vs conn
/proc/net/ip vs stats
/proc/sys/net/ipv4/vs/am droprate
/proc/sys/net/ipv4/vs/amemthresh
/proc/sys/net/ipv4/vs/drop entry
/proc/sys/net/ipv4/vs/drop packet
/proc/sys/net/ipv4/vs/secure tcp
/proc/sys/net/ipv4/vs/timeout close
/proc/sys/net/ipv4/vs/timeout closewait
/proc/sys/net/ipv4/vs/timeout established
/proc/sys/net/ipv4/vs/timeout finwait
/proc/sys/net/ipv4/vs/timeout icmp
/proc/sys/net/ipv4/vs/timeout lastack
/proc/sys/net/ipv4/vs/timeout listen
/proc/sys/net/ipv4/vs/timeout synack
/proc/sys/net/ipv4/vs/timeout synrecv
/proc/sys/net/ipv4/vs/timeout synsent
/proc/sys/net/ipv4/vs/timeout timewait
/proc/sys/net/ipv4/vs/timeout udp