Впервые опубликовано на developerWorks 28.06.2006

Учебник для экзамена LPI 202: Устранение проблем в сети

Администрирование для специалистов (LPIC-2) тема 214

Инструменты конфигурирования сети

Об исправлении проблем в сети

Для исправления проблем настройки сети, вы должны знать как использовать различные инструменты, описываемые в учебниках данной серии; вы также должны быть знакомы с конфигурационными файлами, определяющими состояние и поведение сети. В этом учебнике приводится краткая сводка основных инструментов и конфигурационных файлов, с которыми вы должны быть знакомы, для эфеективных действий по исправлению проблем с сетью.

Для простоты в учебнике инструменты сгруппированы в соответсвии с тем используются ли они больше для настройки сети или для диагностики проблем с сетью. Конечно же на практике эти элементы редко отделены друг от друга.

ifconfig

В Учебнике для экзамена LPI 202 (тема 205): Настройка сети `ifconfig` рассматривается во всех деталях. Эта утилита может и сообщать о статусе сетевых интерфейсов, и позволяет вам изменять настройки этих интерфейсов. В большинстве случаев, когда сеть ведет себя как-то не так -- например, некоторая машина вообще не видна в сети -- первое что следует обычно предпринять это запустить `ifconfig` без параметров. Если она не сможет вывести отчет об активных интерфейсах, то вы можете быть совершенно уверены, что эта локальная машина имеет проблемы в настройке. "Активные" в данном случае означает, что утилита показывает назначеный IP адрес; в большинстве случаев следует ожидать вывода числа пакетов в RX и TX строках:

Листинг 1. Использование ifconfig

```
      eth0    Link encap:Ethernet  HWaddr 00:C0:9F:21:2F:25
              inet addr:192.168.216.90  Bcast:66.98.217.255
Mask:255.255.254.0
              UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
              RX packets:6193735 errors:0 dropped:0 overruns:0 frame:0
              TX packets:6982479 errors:0 dropped:0 overruns:0 carrier:0
```

Попытка активировать интерфейс чем-то вроде `ifconfig eth0 up ...` это хороший первый шаг для определения, что интерфейс может быть активирован (во

многих случаях используются дополнительные опции командной строки).

route

Учебник для экзамена LPI 202 (тема 205): Настройка сети подробно описывает `route`. Эта утилита позволяет легко просматривать и измененять таблицы маршрутизации для локальной машины и локальной сети. Используя `route`, вы можете добавлять и удалять маршруты, определять сетевые маски и шлюзы, а также выполнять множество других задач тонкой настройки.

Для большинства случаев, вызов `route` следует производить из инициализационных сценариев, но в процессе работы по диагностике и исправлению проблем может помочь экспериментирование с настройками маршрутизации (затем вы сможете скопировать удачный вариант в соответствующий стартовый сценарий для последующего использования).

hostname

Эта утилита имеет также псевдонимы для использования а различных аспектах:

- domainname
- nodename
- dnsdomainname
- nisdomainname
- ypdomainname

Используются эти возможности при помощи ключей для самой `hostname`.

`hostname` используется для установки или отображения текущего хоста, домена или имени узла системы. Эти имена используются многими сетевыми программами для идентификации машины. Имя домена используется также и NIS/YP.

dmesg

Утилита `dmesg` позволяет обрабатывать журнал сообщений ядра; она работает совместо с `syslogd`. Доступ к любому процессу ядра, включая те, что связаны с сетью, лучше всего осуществляется при помощи утилиты `dmesg`, часто с наложением фильтрации при помощи другого инструмента вроде `grep`, в качестве ключей `dmesg`.

Ручная установка ARP

Необходимость разбираться с автоматически определенной таблицей ARP записей практически никогда не возникает. Однако, вам может потребоваться вручную изменить кэш ARP, чтобы проверить какие-то предположения об ошибках в сети. Утилита arp позволяет сделать вам это. Ключевыми опциями флагами для утилиты `arp` являются `-d` для удаления, `-s` для установки, и `-f` для установки из файла (стандартным файлом является /etc/ethers).

Например, предположим, что связь с некоторым IP адресом в локальной сети неустойчива или ненадежна. Одной из возможных причин такой ситуации являются несколько машин, настроенных некорректно и использующих один и тот же IP адрес. Когда ARP запрос отправляется по сети Ethernet, то нет определенности, какая машина первой отзовется ARP ответом. Конечным результатом может быть то, что пакеты данных могут доставляться то к одной, то к другой машине.

Первым шагом является использование `arp -n` для проверки имеющихся назначений IP. Если вы обнаружите, что рассматриваемый IP адрес не соответствует корректному Ethernet устройству, то это будет четким сигналом о том, что происходит.

Чтобы преодолеть это возникающий в таком случае разнобой в соответствии IP и сетевого адреса, вы можете насильно указать для проблемного IP его ARP адрес, используя опции `arp -s` (или `-f`). Ручная настройка присвоения адресов будет действовать постоянно, если только специально не использован флаг `temp`. Если ручное ARP присвоение адреса устраняет проблему потери данных, то это четко показывает, что проблема в назначении IP адресов.

Инструменты диагностики сети

netstat

Учебник для экзамена LPI 202 (тема 205): Настройка сети рассматривает `netstat` детально. Эта утилита отображает различную информацию о сетевых соединениях, таблицах маршрутизации, статистику интерфейсов, иммитационные соединения и участие в группах. Кроме этого, `netstat` предоставляет весьма детализированную статистику о пакетах, обработанных различными способами.

Man-страница `netstat` предоставляет информацию о большом количестве доступных ключей и опций. Эта утилита является хорошим инструментом общего назначения для углубления в детали состояния сети на конкретной машине.

ping

Хорошей стартовой точкой для проверки возможности подключения к некоторому узлу с данной машины (по IP адресу или символьному имени) является утилита `ping`. Наряду с определением существует ли маршрут как таковой -- включая разрешение имён через DNS или другим способом при использовании символьного имени -- `ping` предоставляет вам информацию о времени отклика, что может служить индикатором перегрузки сети или задержек маршрутизации. Иногда `ping`

может отображать процент потерянных пакетов, но при практическом применении вы почти всегда будете видеть или 100, или 0 процентов потерянных пакетов для запросов `ping`.

traceroute

Утилита `traceroute` немного напоминает `ping` на стероидах. Вместо того, чтобы просто сообщать о факте наличия маршрута к указанному хосту, `traceroute` сообщает полную информацию о всех переходах, выполненных при прохождении пути, включая время для каждого маршрутизатора. Маршруты с течением времени могут меняться или вследствие динамических изменений в сети Интернет, или вследствии изменений маршрутизации сделанных вами локально. Тем не менее в данный момент времени `traceroute` показывает вам действительный путь следования.

Листинг 2. traceroute показывает действительный путь следования

```
      $ traceroute google.com
      traceroute: Warning: google.com has multiple addresses; using
64.233.187.99
      traceroute to google.com (64.233.187.99), 30 hops max, 38 byte
packets
       1  ev1s-66-98-216-1.ev1servers.net (66.98.216.1)  0.466 ms  0.424
ms  0.323 ms
       2  ivhou-207-218-245-3.ev1.net (207.218.245.3)  0.650 ms  0.452 ms
0.491 ms
       3  ivhou-207-218-223-9.ev1.net (207.218.223.9)  0.497 ms  0.467 ms
0.490 ms
       4  gateway.mfn.com (216.200.251.25)  36.487 ms  1.277 ms  1.156 ms
       5  so-5-0-0.mpr1.atl6.us.above.net (64.125.29.65)  13.824 ms
14.073 ms  13.826 ms
       6  64.124.229.173.google.com (64.124.229.173)  13.786 ms  13.940
ms  14.019 ms
       7  72.14.236.175 (72.14.236.175)  14.783 ms  14.749 ms  14.476 ms
       8  216.239.49.226 (216.239.49.226)  16.651 ms  16.421 ms  17.648
ms
       9  64.233.187.99 (64.233.187.99)  14.816 ms  14.913 ms  14.775 ms
```

host, nslookup и dig

Все три утилиты -- `host`, `nslookup` и `dig` -- используются для опроса записей DNS; большинство их функций перекрываются. Вообще говоря, `nslookup` является улучшенной версией `host`, а `dig` в свою очередь улучшенным `nslookup` (хотя ни одна из трех не имеет полной совместимости сверху или снизу с другими). Все эти инструменты зависят от одних и тех же средств ядра, так что выдаваемые результаты должны быть всегда сходны (исключая случай различия детализации). Например, каждая из трех использовалась для опроса google.com:

Листинг 3. Использование host, nslookup и dig для опроса Google

```
      $ host google.com
      google.com has address 64.233.187.99
```

```
google.com has address 64.233.167.99
google.com has address 72.14.207.99

$ nslookup google.com
Server:         207.218.192.39
Address:        207.218.192.39#53

Non-authoritative answer:
Name:   google.com
Address: 64.233.167.99
Name:   google.com
Address: 72.14.207.99
Name:   google.com
Address: 64.233.187.99

$ dig google.com
; <<>> DiG 9.2.4 <<>> google.com
;; global options:  printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 46137
;; flags: qr rd ra; QUERY: 1, ANSWER: 3, AUTHORITY: 0, ADDITIONAL:
0

;; QUESTION SECTION:
;google.com.                    IN      A

;; ANSWER SECTION:
google.com.             295     IN      A       64.233.167.99
google.com.             295     IN      A       72.14.207.99
google.com.             295     IN      A       64.233.187.99

;; Query time: 16 msec
;; SERVER: 207.218.192.39#53(207.218.192.39)
;; WHEN: Mon Apr 17 01:08:42 2006
;; MSG SIZE  rcvd: 76
```

Файлы настройки сети

/etc/network/ и /etc/sysconfig/network-scripts/

Каталог /etc/network/ во многих дистрибутивах Linux содержит различные данные для текущей сети, особенно в файле /etc/network/interfaces. Различные утилиты, особенно `ifup` и `ifdown` (или `iwup` и `iwdown` для беспроводных интерфейсов) в некоторых дистрибутивах находятся в /etc/sysconfig/network-scripts/ (но те же скрипты в вашем дистрибутиве могут находиться где-то в другом месте).

/var/log/syslog и /var/log/messages

Сообщения от ядра или средства `syslogd` записываются в файлы журналов /var/log/syslog и /var/log/messages. Учебник для экзамена LPI 201 (тема 211): Обслуживание системы детально рассматривает журналирование системы. Обычно

для проверки журналов (log-файлов) используется утилита `dmesg`.

/etc/resolv.conf

Учебник для экзамена LPI 202 (тема 207): Служба имен доменов (Domain Name System) детально рассматривает /etc/resolv.conf. Вообще говоря, этот файл просто содержит необходимую для нахождения доменных имен серверов. Он может быть настроен вручную или посредством динамического метода типа RIP, DHCP или NIS.

/etc/hosts

Файл /etc/hosts обычно является тем, что система Linux просматривает в первую очередь при попытке распознать символьное имя хоста. Вы можете добавить в него записи или для пропуска поиска DNS (или иногда средств YP или NIS), или для задания имени хоста, которые не доступны через DNS, часто вследствии того, что они имеют прямые имена в локальной сети. Смотри пример в Листинге 4

Листинг 4. /etc/hosts, место для разрешения символьных имен хостов

```
$ cat /etc/hosts
# Set some local addresses
127.0.0.1         localhost
255.255.255.255   broadcasthost
192.168.2.1       artemis.gnosis.lan
192.168.2.2       bacchus.gnosis.lan
# Set undesirable site patterns to loopback
127.0.0.1       *.doubleclick.com
127.0.0.1       *.advertising.com
127.0.0.1       *.valueclick.com
```

/etc/hostname и /etc/HOSTNAME

Файл /etc/HOSTNAME (на некоторых системах не заглавными буквами) иногда используется для символьного имени локального хоста, известного в сети. Однако, использование этого файла в различных дистрибутивах различается; вообще говоря, /etc/hosts используется только в новых дистрибутивах.

/etc/hosts.allow и /etc/hosts.deny

Учебник для экзамена LPI 201 (тема 209): Совместное использование файлов и сервисов и учебник для экзамена LPI 202 (тема 212): Безопасность системы рассматривают файлы /etc/hosts.allow и /etc/hosts.deny детально. Эти конфигурационные файлы используются для позитивных и негативных списков контроля доступа различными сетевыми инструментами. Читайте man-страницы этих конфигурационных файлов, чтобы получить больше информации о спецификациях шаблонов, диапазонов и специальных запретов.

Если после начальной настройки безопасности системы соединения нет, хотя кажется, что оно должно работать, стоит начать анализ с проверки содержимого этих файлов. Вообще, проверка элементов управления доступом при анализе причин проблем следует сразу за проверкой основных интерфейсов и информации о маршрутизации. То есть, если вы вообще не можете "достучаться" до некоторого хоста (или он не может обратиться к вам), то не имеет значения, имеет ли хост запрет на использование предоставляемого вами сервиса. Но причиной отдельных сбоев соединения и сервисов обслуживания часто могут быть элементы управления доступом.

Заключение

Используйте преимущества каждого ресурса

Вероятно лучшим ресурсом дополнительной информации по темам рассмотренным в данном учебнике является вся эта серия уроков. Практически все затронутые здесь темы были детально описаны в предыдущих учебниках.

Очень мало тех, кто создает руководства пошагового исправления не работающей сети в Linux. Одним из них, и весьма приличным, является "Simple Network Troubleshooting [Простое исправление проблем в сети]." Подобное быстрое руководство от Debian "How To Set Up A Linux Network [Как настроить сеть в Linux]." Поскольку учебники появляются, исчезают и обновляются по различным схемам, по мере изменения дистрибутивов и команд, вы всегда можете использовать поиск в Интернет, чтобы найти ресурс доступный в настоящее время.