리눅스 서버 네트워크 관리

리눅스 서버의 네트워크 설정 관련 파일들

ㅇ 리눅스서버의 네트워크 설정 파일들

- 기본게이트웨이 설정파일(네트워크 기본 설정파일)
  /etc/sysconfig/network
- 이더넷설정파일
  /etc/sysconfig/network-scripts/ifcfg-eth0
  /etc/sysconfig/network-scripts/ifcfg-eth1
  ……
- 사용할 네임서버정보 : /etc/resolv.conf
- 로컬호스트파일 : /etc/hosts

ㅇ 네트워크 설정 명령어 및 스크립트파일들

- 네트워크 스크립트파일 : /etc/rc.d/init.d/network restart
- 이더넷 설정 : ifconfig
- 게이트웨이 설정과 네트워크 경로설정 : route
- 통신 테스트 : ping
- 통신경로확인 : traceroute
- 네트워크 연결상태 종합 점검 : netstat
- 이더넷카드 속도설정과 전송모드 설정 : ethtool
- TCP패킷캡처 및 패킷 모니터링 : tcpdump
- 네트워크 인터페이스 설정확인 및 변경 : mii-tool

리눅스 서버에 IP주소할당 및 IP주소 변경

ㅇ 네트워크 설정파일을 이용한 IP주소 할당 및 변경

- /etc/sysconfig/network
- /etc/sysconfig/network-scripts/ifcfg-eth0
  /etc/sysconfig/network-scripts/ifcfg-eth1

- 설정완료후 : /etc/rc.d/init.d/network restart

ㅇ 명령어를 이용한 IP주소 할당 및 변경

- ifconfig eth0 192.168.0.253 netmask 255.255.255.0 broadcast 192.168.0.255 up
- route add default gw 192.168.0.254 dev eth0

ㅇ 유틸리티를 이용한 IP주소 할당 및 변경

- netconfig
- system-config-network
- redhat-config-network

한 개의 이더넷에 여러 개의 IP주소 할당

○ I P 앨리어싱

물리적으로 한 개의 이더넷에 여러 개의 가상 이더넷장치파일을 만들어서 여러 개의 IP주소를 할당하여 사용하는 것.

○ 1단계 : 현재 네트워크 설정상태 확인

- ifconfig
- /etc/sysconfig/network
- /etc/sysconfig/network-scripts/ifcfg-eth0

○ 2단계 : 여러 개의 가상이더넷설정파일 생성 및 생성한 파일 설정

- /etc/sysconfig/network-scripts/ifcfg-eth0:0
- /etc/sysconfig/network-scripts/ifcfg-eth0:1
- /etc/sysconfig/network-scripts/ifcfg-eth0:2

  .....

○ 네트워크 스크립트파일 재시작

- /etc/rc.d/init.d/network restart

리눅스 서버의 라우팅테이블 설정 및 관리하기

ㅇ 라우팅테이블 확인하기와 라우팅테이블 이해하기

```
[root@fileserver ~]# route
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
192.168.0.0     *               255.255.255.0   U     0      0        0 eth0
169.254.0.0     *               255.255.0.0     U     0      0        0 lo
127.0.0.0       *               255.0.0.0       U     0      0        0 lo
default         192.168.0.1     0.0.0.0         UG    0      0        0 eth0
[root@fileserver ~]#
```

*** 규칙**

1. 차례대로 한행씩 읽어들임.
2. 보낼 데이터의 Destination IP Address와 Genmask(SubnetMask) IP Address와의 AND연산을 하여 그 결과가 해당행의 Destination과 같을 경우 해당행의 Iface에 지정된 장치로 보내게됨.
3. default는 기본게이트웨이를 의미함. 즉 0.0.0.0과 같음.
4. Iface값이 lo인 것은 자기자신과의 통신에 사용되는 loop back 데이터 처리용 인터페이스.

예) 목적지주소가 192.168.3.101인 패킷의 라우팅경를 설명하시오.

ㅇ 기본게이트웨이 설정하기

- route add default gw 192.168.0.254 dev eth0

ㅇ 네트워크 라우팅 경로 추가하기

- route add –net 192.168.1.0 netmask 255.255.255.0 dev eth1

리눅스 서버의 네트워크 경로 상태 점검하기

ㅇ 경로 점검 명령어

- 특정 호스트 또는 특정 네트워크장비까지의 통신여부 확인 : ping
- 특정 호스트 또는 특정 네트워크장비까지의 통신경로 확인 : traceroute

ㅇ 대상서버(장비) ping 테스트

- 1회 ping테스트시 총패킷사이즈 = ICMP헤드(8byte) + 패킷사이즈

- 사용예
  . ping 192.168.0.1

```
[root@edu ~]# ping 192.168.0.100
PING 192.168.0.100 (192.168.0.100) 56(84) bytes of data.
64 bytes from 192.168.0.100: icmp_seq=0 ttl=64 time=1.33 ms
```

  . ping –c 4 –s 1000 192.168.0.160

ㅇ 통신경로(구간) 점검 : traceroute

- 대상호스트(서버)까지 어떤 구간을 거쳐서 통신이 이루어 지는가를 확인
- 대상호스트(서버)까지 몇 개의 HOP수(대부분 게이트웨이)를 거쳐가는가를 확인
- 대상호스트(서버)까지의 구간에 통신장애가 존재하는가를 확인
- 사용예
  . traceroute 211.220.220.111
  . traceroute www.superuser.co.kr

리눅스 서버 호스트네임 변경하기

ㅇ 호스트네임 설정파일

- /etc/sysconfig/network 파일내에 HOSTNAME이라는 행에 설정함.

ㅇ 호스트네임 설정 명령어

- 호스트네임저장하고 있는 쉘변수 : HOSTNAME

- 현재 호스트네임 확인
  . hostname
  . echo $HOSTNAME

- 새로운 호스트네임 설정 : hostname 새로운호스트명

리눅스 서버의 네트워크 연결상태 전체점검

ㅇ netstat로 확인할 수 있는 것은?

- 네트워크연결 상태
  . 어떤IP주소를 가진 곳에서 연결되어 어떤서비스의 몇번 포트를 사용중인가? 등
- 라우팅테이블 확인
- 프로토콜별 서비스된 통계
- 열려져있는 포트 및 서비스중인 프로세스들의 상태정보, 그리고 PID정보들
- netstat으로 확인가능한 서버와 클라이언트의 상태정보 문자와 의미 (결과중 state값)
  . LISTEN : 서버에서 관련 서비스(데몬)이 서비스가 가능한 상태. 서비스 요청을 기다리고 있는 상태.
  . SYS_SENT : 클라이언트가 서버에게 SYN패킷을 보낸후 연결을 요청한 상태.
  . SYN_RECEIVED : 서버가 클라이언트의 SYN패킷으로 서비스 요청을 받은 후에 이에 대한 응답으로 SYN/ACK패킷을 보내고, 클라이언트에게 ACK패킷을 받기를 기다리는 상태.
  . ESTABLISHED : 서버와 클라이언트간의 3 way handshake(SYN->SYN/ACK->ACK)완료 후에 실제 데이터를 교환하고 있는 상태.
  . FIN_WAIT1, CLOSE_WAIT, FIN_WAIT2 : 연결종료를 위해 종료요청을 받은 후의 종료과정 상태.
  . CLOSING : 전송된 메시지가 유실된 상태.
  . TIME_WAIT : 연결종료 후 일정시간동안 유지하고 있는상태(일정시간 후 자동 종료됨)
  . CLOSED : 서버와 클라이언트간의 연결이 완전히 종료된 상태.

ㅇ netstat의 사용예

- 라우팅테이블 정보 확인 : netstat –nr
- 각프로토콜들에 대한 통계정보 : netstat –s
- 현재 LISTEN된 소켓정보와 LISTEN되지 않은 소켓정보 모두를 보여줌 : netstat -an
- 현재 LISTEN된 소켓정보와 LISTEN되지 않은 소켓정보를 PID와 함께 보여줌 : netstat –atp
- SYN Flooding공격여부 가능성 점검 : netstat –an | grep SYN_RECV

* 클라이언트 ---------- 서버 *

NIC의 상태확인과 속도 및 전송모드 설정

ㅇ NIC 확인과 설정

- 속도 : 10M 또는 100M등
  . NIC의 속도설정은 대부분 auto모드로 설정되어 있음.
- 전송모드 : half duplex 또는 full duplex
- 사용명령어 : ethtool
  mii-tool

ㅇ 사용예

- NIC설정확인 : ethtool eth0
- NIC설정변경
  ethtool –s eth0 speed 100 duplex full autoneg off

ㅇ 참고 : mii-tool

- 네트워크인터페이스의 상태확인, 전송모드(전이중, 반이중), auto-negotiation설정등 확인
- 사용예
  . 장착된 모든 NIC들의 설정상태 확인 : mii-tool
  . 특정 NIC만의 설정상태 확인 : mii-tool eth0
  . 상세한 설정상태 확인 : mii-tool –v
  mii-tool –v eth0

패킷캡처를 이용한 패킷 모니터링하기

○ 패킷캡쳐의 의미와 목적
- 특정 네트워크 인터페이스의 패킷을 캡쳐할 수 있음.
- 캡쳐후 결과를 분석하면 네트워크와 이더넷의 이상유무를 확인할 수 있음.
- ftp나 telnet등과 같은 암호화되지 않은 프로토콜 서비스등에 의해 발생되는 패킷을 캡쳐하여 불법정보(id와 password등)를 확인하면 크래킹도구로도 악용될 수 있음.(일종의 스니핑)

○사용예
- eht0 인터페이스를 거쳐가는 패킷 헤드를 확인
  tcpdump –i eth0

- 캡쳐결과를 특정 파일로 저장하기
  tcpdump –i eth0 –w traffic.txt

- 지정한 개수만큼만 캡쳐하기
  tcpdump –i eth0 –c 20

- 특정호스트와 특정포트번호로 서비스되는 패킷 전체를 캡처하여 특정파일에 저장하기
  tcpdump –i eth0 –w traffic –s 1500 tcp port 22 and host 192.168.0.100

  저장한 파일을 텍스트포맷 확인하기
  tcpdump –r traffic.txt

  결과파일을 ASCII모드로 확인하기
  tcpdump –Xqnr traffic