DNS기초에서 보안까지 !!!

여행을떠나다

소개글

DNS에 대해 쉽게 이해할수 있도록 설명했습니다.

네이버 DNS전문가카페 http://cafe.naver.com/dnspro

목차

1.1 DNS개요

2011.04.10 18:52

여기서부터 DNS 기본 이론 자료입니다.

이론적인 내용이 많으니 그냥 한번 쭉~ 읽고 지나가시면 될거 같습니다. 프린트까지는 하실필요는 없을거 같구요.

1.1 DNS 개요

도메인 네임 시스템(DNS, Domain Name System)이란 name(이름)과 IP주소를 매핑하여 주는 거대한 분산 네이밍 시스템입니다.
인터넷에서 사용되는 IP(Internet Protocol), 그리고 IP의 상위에서 동작하는 어플리케이션들은 210.103.175.2와 같이 표현되는 IP주소만을 인식하게 되는데, 이러한 IP주소는 기계 입장에서는 해석하기 수월하지만, 기억하기 어렵고, IP주소만으로는 서비스 유형을 예측하기 어렵다는 단점이 있습니다.

따라서 인터넷의 도입 시절인 ARPAnet 시절부터 IP주소를 이름으로 명명하여 사용하고자 하는 노력이 시도되었고, 많은 시행착오를 거쳐 지금의 DNS 메커니즘으로 발전하였습니다.

1.1.1 ARPAnet 과 HOSTS.TXT

1970년대의 ARPAnet은 수백 개도 안되는 호스트들로 이루어진 작은 규모였습니다.
ARPAnet에 연결된 모든 호스트들에 대하여 이름과 주소간의 매핑 정보는 HOSTS.TXT라는 하나의 파일에 담겨있었습니다.
이 HOSTS.TXT파일은 일정 주기마다 배포되었습니다. 그러나 ARPAnet이 성장해감에 따라 HOSTS.TXT파일의 크기도 함께 증가하였고, 갱신하기 위해 발생하는 트래픽은 더더욱 빠르게 증가하였습니다.

결국 네트워크 트래픽의 증가와 일관성 없는 이름 할당으로 인한 충돌 등의 문제로 인해 새로운 시스템이 필요하게 되었습니다.

1.1.2 DNS의 출현

ARPAnet 시절에는 호스트의 수가 많지 않았기에 NIC(Network Information Center)으로부터 일정 주기마다 호스트 명단 파일(HOSTS.TXT)을 받아 /etc/hosts에 저장하여 사용하였습니다.
그러나 점차 인터넷의 규모와 호스트 수가 증가함에 따라 새로운 이름 명명 체제의 필요성이 대두되었고, 1983년 Paul Mockapetris가 RFC882, RFC883(현재는 RFC1034로 대체됨)에 새로운 명명 체제에 대한 구현을 공식 발표하며, 크게 네임스페이스의 계층 구조, 분산 데이터베이스, Email 라우팅 개선을 주안점으로 DNS가 탄생하였습니다.

새로운 시스템은 데이터를 로컬하게 관리할 수 있어야 하고 동시에 글로벌하게 이용할 수도 있어야 했습니다.
관리의 분산화는 단일 호스트일 때의 병목 현상 및 트래픽의 문제를 없앨 수 있고 로컬 관리는 데이터를 매우 쉽게 최신으로 유지할 수 있습

니다.

호스트의 이름을 짓기 위해서 반드시 계층적 이름 공간을 이용하므로 이는 이름의 고유성을 보장할 수 있습니다. 이러한 배경에 따라 현재의 DNS가 구축되기에 이르게 되었습니다.

[DNS교육] DNS 장애처리 및 보안설정 신청 : http://www.bpan.com/edu_new/edu_lec/49

1.2 DNS BIND 소개

2011.04.10 18:53

1.2 DNS BIND 소개

1.2.1 BIND 의 역사

도메인 네임 시스템을 처음 구현한 것은 폴 모카페트리스(Paul Mockapetris)가 개발한 JEEVES입니다. 그 뒤에 케빈 던랩(Kevic Dunlap)이 4.3BSD 유닉스용으로 작성한 BIND(Berkeley Internet Name Domain)이며, 현재 ISC(Internet Systems Consortium)에서 관리하고 있습니다
자세한 히스토리는 https://www.isc.org/software/bind 를 참조하십시오.

1.2.2 버전고르기

현재는 BIND9가 많이 사용되는 추세이며, 최근 리눅스OS는 DNS설치시 BIND9 버전만 설치되고 있습니다.

BIND 9.5 Administrator Reference Manual
https://www.isc.org/software/bind/documentation/arm95

BIND 9.4 Administrator Reference Manual,
https://www.isc.org/software/bind/documentation/arm94

대부분의 상용 유닉스 제작사들은 BIND를 다른 TCP/IP 네트워크 소프트웨어에 포함하여 판매하고 있습니다.
리눅스,유닉스에 BIND가 포함되어 있지 않거나 최신 버전의 BIND를 구하고 싶은 경우에도 소스 코드를 언제라도 구할 수 있으며, 무료로 배포되고 있습니다.

운영체제에 BIND가 이미 설치되어 있는데도 최신 버전의 BIND를 구해 설치해야 하는 이유는 최신 버전이 네임 서버 공격에 대해 패치 되어 있고, 향상된 보안기능과 고급기능을 지원함으로 BIND 관리에 도움을 주기 때문입니다. 그리고 BIND 4, BIND 8, BIND 9의 설정 구문 문법이 다르기 때문에 새로 배우는 것이 필요합니다.
참고로 현재 BIND4는 거의 사용되고 있지 않으며, BIND 8도 2007년 중순부터 더이상 패치가 되지 않습니다.

[DNS교육] DNS 장애처리 및 보안설정 신청 : http://www.bpan.com/edu_new/edu_lec/49

1.1 기초 DNS 이론

2011.04.10 18:54

1.1 기초 DNS 이론

1.1.1 네임공간(Namespace)

ARPANET의 중앙 관리 체제에서는 하나의 파일로 모든 호스트들을 관리하였지만, DNS에서는 이것을 각 **도메인별로 트리화 하여 관리합니다.**
디렉토리 구조와 유사함을 알 수 있는데, Root domain(도트로 표시되는)은 Top level 도메인에 관한 정보를, Top level 도메인은 그 하위 도메인에 관한 정보를 유지/관리하는 구조를 취합니다. 이러한 정보의 계층구조로 인하여 정보는 각 도메인의 네임서버(NS:Name Server)로 분산, 관리됩니다.
예로 YAHOO.COM 도메인은 COM 네임서버에 등록되어 있고, WWW.YAHOO.COM은 YAHOO.COM 네임서버에 등록, 관리됩니다.
따라서 AV.YAHOO.COM을 등록하기 위해서는 YAHOO.COM 도메인을 관리하는 네임서버의 관련 레코드만을 수정함으로써 가능합니다. 이러한 위임구조는 증가하는 인터넷 호스트에 대한 관리를 효율적으로 가능하게 해줍니다.

네임공간의 동작

1) PC가 www.aaa.com에 대해 DNS에게 질의하면
2) DNS 〈-〉 ROOT // root는 .com에 대한정보만 준다
3) DNS 〈-〉 GTLD(.COM Root등) // .com root는 aaa.com에 대한 네임서버ip를 알려준다.
4) DNS 〈-〉 네임서버 // 네임서버는 www.aaa.com ip를 DNS에 알려준다.
5) DNS는 PC에 www.aaa.com에 대한 ip를 알려준다.
6) PC 〈-〉 웹서버 이렇게 가게됩니다.

이런 공간을 네임공간 이라고합니다.

1.1.2 노드와 레이블(Nodes와 Labels)

DNS 데이터베이스의 구조는 유닉스 파일시스템과 매우 유사한 역트리 구조입니다. 꼭대기에 루트 노드가 있고, 트리의 각 노드는 텍스트 레이블을 포함하고 있으며, 관련있는 노드를
'부모-자식' 관계로 정의하는데 이 개념은 파일시스템의 '상대 경로명' 과 비슷합니다. 아무 것도 없는 null 레이블(" ")은 루트 노드를 의미하며 텍스트에서 루트 노드는 점(.)하나로 나타냅니다. 반면 유닉스 파일시스템에서는 루트를 슬래시(/)로 표현합니다.

구조 설명

Root(.)
-〉 .com root (GTLD)
-〉 네임서버 이러한 단계를 의미하는것입니다.

Windows c:₩
-〉 c:₩windows
-〉 c:₩windows₩system32 이런것 처럼요.

1.1.3 도메인과 서브도메인

각 노드는 전체 트리의 새로운 서브 트리의 루트도 되며, 이러한 서브 트리 각각은 유닉스 파일시스템에서는 '디렉토리'를 도메인 네임 시스템에서는 '도메인'을 나타냅니다.
각 도메인이나 디렉토리를 더 작게 나눌 수 있는데, 이것을 DNS에서는 서브 도메인이라고 하고 서브 디렉토리처럼 부모 도메인의 자식으로 그려집니다. DNS에서의 도메인 네임은 도메인의 루트에 해당하는 노드에서 전체 트리 루트까지의 노드 레이블을 나열한 것으로 '.'으로 연결되어 있습니다. 트리의 제일 하단에 있는 잎 노드(leaf node)에 해당하는 도메인 네임은 개별 호스트를 나타내며, 네트워크 주소, 하드웨어 정보, 그리고 메일 라우팅 정보 등을 가리킵니다.

설명: korea.com 이게 도메인이구요..
pusan.korear.com 이런게 서브도메인이라고 보시면 될거 같습니다.

1.1.4 위임(delegation)과 영역(zone)

어떤 도메인을 관리하는 기관은 도메인을 여러 서브 도메인으로 나누고 각 서브 도메인을 다른 기관에 위임할 수가 있습니다. 그리고 이것은 한 기관이 해당 서브 도메인의 모든 데이터를 관리하는 책임을 갖게 되어 그 기관이 데이터를 자유롭게 변경하거나 서브 도메인을 더욱 작은 서브 도메인으로 나눠서 다른 곳에 위임할 수 있습니다. 부모 도메인은 서브 도메인의 데이터가 있는 곳을 가리키는 포인터만 갖게 됩니다. 도메인 네임 공간에 대한 정보를 저장하는 프로그램을 네임 서버라고 합니다. 네임 서버는 영역(zone)이라 불리는 도메인 네임 공간의 일부분에 대한 완벽한 정보를 갖고 있고 영역 정보는 파일로부터 읽어 들이거나 다른 네임 서버로부터 읽어 들입니다.

설명: korea.com 이 도메인인데..
분당,서울에 캠퍼스(budang.korea.com pusan.korea.com) 이 있으면..
일일이 서울에서 elec.pusan.korea.com sansu.bundang.korea.com를 등록하지 않고..

분당 캠퍼스에 budang.korea.com 네임서버를 만들고, 서울에서 budang.korea.com에 대한 권한을 분당에 넘겨주는것을 위임이라고 합니다. 보통 CNAME으로 위임하거나 NS위임중 하나를 합니다.

위임이 되고 나면 분당 네임서버(budang.korea.com)에서 xxx..budang.korea.com 처럼 xxx는 마음데로 추가가능하고, 관리가 가능합니다.
game1.budang.korea.com 이나.. eng1.budang.korea.com 처럼..

실무에서 위임을 하는경우는 CDN업체에 파일업로드서브도메인이나 이미지서브도메인을 위임할때 주로 사용된다.
CDN업체의 GSLB장비(3DNS,GTM장비,아라GSLB)로 위임할때 주로 사용한다.

1.1.5 마스터 (Master) 와 슬레이브(Slave) 네임서버

영역의 주 마스터 네임 서버는 파일로부터 영역에 대한 데이터를 읽습니다. 보조 마스터 네임 서버는 그 영역에 대한 권한을 갖고 있는 다른 마스터 서버로부터 영역 데이터를 얻어오며, 다른 보조 마스터로부터 영역 데이터를 가져올 수 있습니다. 영역 데이터를 긁어오는데 이것을 영역 전송(zone transfer)라고 합니다. 슬레이브(주마스터의 데이터에 의존) 서버는 낮은 급수의 네임서버가 아니며, DNS 는 두 종류의 네임서버를 제공함으로써 관리를 편하게 합니다.
네임 서버를 여러 개 두면 장애가 났을 때도 문제가 없고, 네임 서버의 부하를 덜 수 있으며, 영역 내의 모든 호스트가 가까운 곳에 있는 네임 서버를 이용할 수도 있게 됩니다.

설명:
Master는 www, mail 등 호스트를 추가할수 있구요..
Slave는 마스터정보를 받아와 동일하게 유지하며 서비스하는것입니다.

실무에서 도메인등록시 네임서버를 2개로 등록하는 이유는 Master나 Slave가 동일하게 동작하고,
로드 분산하므로 1개가 다운 되더라도 정상서비스가 됩니다.

1.1.6 리졸버(Resolver)

도메인 네임 공간의 정보가 필요한 호스트 내의 프로그램들은 리졸버를 이용합니다. 이 리졸버는 네임 서버에 질의(query)를 보내고, 응답(RR 레코드 또는 Error)를 해석한 뒤 요청했던 프로그램에 정보를 되돌려 줍니다. 텔넷이나 ftp 등의 프로그램에 링크되는 라이브러리 루틴의 집합입니다. 이러한 종류의 리졸버를 stub(스텁) 리졸버라고 부릅니다.
Stub 리졸버 : 질의 생성 -〉 서버 전송 -〉 응답 기다림 -〉 응답 없으면 재질의 전송

설명:
리졸버는 PC라고 생각하면 됩니다.
리졸버(resolver)는 네임 서버를 엑세스하는 클라이언트입니다.

1.1.7 이름 분해 (Name Resolution)

네임 서버는 자신이 권한을 갖는 영역에 대한 데이터만 알려주는 것은 아니고, 권한이 없는 데이터도 도메인 네임 공간을 뒤져서 찾을 수 있습니다. 이러한 과정을 이름 분해 또는 간단히 resolution 이라고 합니다. 도메인 네임과 루트 네임 서버의 주소는 네임 서버가 어느 지점에서부터 정보를 찾아야 하는지에 대한 정보입니다.

설명:

PC에서 로컬 DNS 〈-〉(Root , GTLD (.com root등) , 네임서버)등 이러한 질의 응답과정을 레졸루션이라고 한다.

1.1.8 Recursive (재귀적) 질의, Iterative 질의

네임서버가 Recursive 모드로 동작할 때에는, 클라이언트(이를 Stub Resolver 라 합니다.)의 요청에 대해 Namespace를 검색한후 결과를 전달한다. 하지만 Iterative 모드에서는 알 수 없는 질의(자신이 관리하지 않는 도메인에 대한 요청)에 대해, 응답 가능한 NS의 목록을 전달합니다.

네임서버는 Recursive 모드로 동작하며, Iterative 모드는 루트서버와 같이 네임서버를 위한 네임서버(네임서버간의 통신에는 Iterative 모드가 사용됨)에서 과다한 트래픽을 막기위해 사용한다. 또한, 클라이언트는 Iterative 모드로 설정된 네임서버를 사용할 수 없으므로, 네임서버 목록(예:resolv.conf, 윈도우의 DNS 찾기목록)에 추가하여서는 안됩니다. BIND-4에서는 부트파일에 'options no-recursion'을 추가함으로써, Iterative 모드로 전환할 수 있고, BIND8, 9의 경우엔 options 엔트리에 'recursion no;'를 설정합니다.

1.1.9 캐싱(Caching)

캐싱은 resolution의 속도를 높이는 역할 이외에도, 루트 네임 서버에 질의를 보내야할 필요를 덜어줍니다. 그럼으로써 루트 네임 서버에 너무 의존하지 않아도 되고 아울러 루트 네임 서버가 겪는 수많은 부담을 덜어줄 수도 있습니다. Bind 4.9, 버전 8, 버전 9 에서는 네임 서버들이 부정적 캐싱(negative caching)을 할 수 있는데 네임 서버가 질의한 도메인 네임이나 데이터 종류가 존재하지 않는다고 대답하면, 로컬 네임 서버는 그 정보도 캐시에 임시로 저장합니다. 네임 서버는 긍정적인 응답이든 부정적인 응답이든 모두 캐싱할 수 있어서, 리졸버에게 바로 대답을 알려준다. 심지어 응답을 캐싱하고 있지 않더라도 학습을 통해 그 영역의 권한을 갖는 네임 서버를 알고 있을 수 있기 때문에 복잡한 과정을 거치지 않고 그 네임 서버에 바로 직접 물어볼 수 있습니다.

설명:
PC에 캐싱된다 라는것, DNS에 캐싱된다라는거 그런의미입니다.
다시 물어보지 않고 로컬에 정보를 일정시간 가지고 있다가, 질의시 로컬에서 바로 답변을 주는것이죠.

1.1.10 네임 서버 왕복 시간(RTT, roundtrip time)

어떤 영역에 대한 권한을 갖는 네임 서버가 여러 개 있을 때, BIND 네임 서버는 왕복시간(RTT, roundtrip time) 이라는 척도를 이용해 그 중의 하나를 선택합니다. 왕복 시간은 원격 네임 서버가 질의에 응답하는 데 걸리는 시간입니다. BIND 네임 서버는 원격 네임 서버에게 질의를 보내면서 내부의 초시계를 시작시킵니다. 이 초시계는 원격 네임 서버로부터 응답을 받으면 멈추며 소요 시간이 기록됩니다. 그래서 여러 원격 네임 서버 중에서 하나를 선택해야 하는 경우에는 가장 작은 RTT 값을 갖는 네임 서버를 고릅니다. 어떤 원격 네임 서버에도 질의를 보내지 않은 초기 상황에는 임의의 RTT 값이 할당되고, 시간이 흐르면서 더 큰 RTT 값으로 대치되어 주어진 영역에 대한 네임 서버 모두에 적어도 한번씩은 질의를 보내게 됩니다.

설명:

네임서버가 여러대가 있는데, DNS에서 찾아갈때 쉽게 ping같은거 때려보고 가까운데 간다는거로 생각하면 어떨까합니다.
ping응답시간같은걸 RTT알고리즘이라고 생각하면 될거 같습니다.
RTT알고리즘은 한번 질의자에게게는 가중치를 주어. 그다음 질의시 다른서버에 질의하여 분산되도록 한다고 보시면 될거 같습니다.

[DNS교육] DNS 장애처리 및 보안설정 신청 : http://www.bpan.com/edu_new/edu_lec/49

1.1 DNS 일반 도메인

2011.04.10 18:57

1.1 DNS 일반 도메인

1.1.1 일반 최상위 도메인 (Generic Top-level Domain)

일반 최상위도메인을 GTLD라고 한다. 일반적으로 .com 이 가장 많이 사용합니다. 아시죠^^

인터넷 네임 공간은 구조별로 7개의 최상위 레벨 도메인으로 나뉩니다.
.Com 영리를 목적으로 하는 기관(commercial organization) 예) hp.com sun.com ibm.com
.edu 교육 기관(educational organization) 예) Berkeley.edu, purdue.edu
.gov 정부 기관(government organization) 예) nasa.gov, nsf.gov
.mil 군사 기관(military organization) 예) army.mil, navy.mil
.net 네트워크 기관(networking organization), 1996년 이후 등록 제한이 없어짐 예) nsf.net
.org 비영리 기관(noncommercial organization), 1996년 이후 등록 제한이 없어짐 예) eff.org
.int 국제적인 기관(international organization) 예) nato.int

2001년 이후로 name, biz, info, pro, aero, coop, museum 이 추가되었습니다.
도메인 네임 공식 관리는 ICANN(Internet Corporation for Assigned Names and Numbers) 에서 맡고 있습니다.

1.1.2 국가코드 최상위도메인 (Country-Code Top-Level Domain)

국가 도메인을 CC TLD 라고하고, 우리나라는 .kr 이 사용되고 있다.

.KR Korea, Republic of 대한민국
.AU Australia 호주
.DE Germany 독일
.JP Japan 일본
.TW Taiwan, Province of China 대만
.US United States 미국

1.1.3 최상위 도메인 기관

도메인등록 역활대행(레지스트라)로는 아이네임즈,가비아,후이즈.IBI 등이 있습니다.

1999년 봄 이전에는 NSI(Network Solutions Inc)만이 com net org edu의 레지스트리이자 독점 레지스트라였습니다. 도메인 네임 공간을 관리하는 단체인 ICANN 은 1999년 6월부터 com, net, org에 대한 레지스트라에 경쟁을 도입해서 com,net org 레지스트라가 다수 존재합니다.

1.1.4 Registry와 Registrar

Registry (레지스트리)

Internet Governance인 ICANN에게서 ccTLD 또는 gTLD의 SLD(Second level Domain) 에 대한 운영 및 Resolution에 대한 기능을 이양 받아 계약기관 동안 안정적인 운영을 담당하게 됩니다.

모든 Registry Data를 보관해야 하며 최소 하루 안에 업데이트를 하고, whois 서비스를 제공하고 Registrar에 Registration Protocol을 제공합니다.

- RRP-Registry : Registrar에게 도메인 정보(Registrar, Domain, Name Server, 신규일, 만료일) 만을 받게됨.
- EPP-Registry : Registrar 가 가진 모든 도메인 정보를 Registry가 가지게 됨.
- 참고 : http://www.icann.org/registries/agreements.htm

Registrar (레지스트라)

아이네임즈, 가비아, IBI등 '도메인등록 역할대행' 기관을 "레지스트라" 라고 한다.

1999년 봄 이전에는 NSI(Network Solutions Inc)만이 com net org edu의 레지스트리이자 독점 레지스트라였다.
도메인 네임 공간을 관리하는 단체인 ICANN 은 1999년 6월부터 com, net, org에 대한 레지스트라에 경쟁을 도입해서
com,net org 레지스트라가 다수 존재한다.

Registrant로부터 직접 SLD의 등록을 받아 등록 서비스를 유지
SLD의 등록/변경/삭제와 관련된 서비스, Whois서비스, 도메인 Data에 대한 정확성 유지, ICANN에 약 18000불, Registry에 도메인당 약6불 (도메인마다 다름)

짧은시간에 이해하시려면 교육을 들으시면 됩니다.^^
[DNS교육] DNS 장애처리 및 보안설정 신청 : http://www.bpan.com/edu_new/edu_lec/49

1.1 DNS기초 IP (Internet Protocol)

2011.04.10 18:58

1.1 IP (Internet Protocol)

1.1.1 위치 및 할당정책 (Allocation & Assign 정책)

전세계가 RFC2050 공통의 원칙, Host 수와 네트웍 구성에 좌우되며 낭비되는 IP 주소가 없도록 할당해야 합니다.
세부적으로 IP는 대여개념, 하나의 가입기관에 종속기관이 포함되고, whois정보는 사용권리를 의미, 인터넷 라우팅 보장 불가합니다.
IP신청은 반드시 하나의 Internet Registry에서 받아야 합니다. 1년이내 IP추가 할당 신청은 원칙적으로 불가하며, IP할당과 관련된 모든 자료 제출 요구시 반드시 응해야 합니다. IP절약기술(CIDR, VLSM등)을 반드시 적용하여, 개인 사용자에 대한 static 할당 불가합니다. 가상서버 세팅시 IP할당 불가합니다.

1.1.2 IP 관리기관

ARIN http://www.arin.net/whois/index.html
APNIC http://whois.apnic.net <- 아시아 관리기관
RIPE NCC http://www.ripe.net/cgi-bin/whois
AfriNIC

1.1.3 CIDR (Classless Inter-Domain Routing, 싸이더)

인터넷 32비트 주소 공간은 A클래스, B클래스, C클래스라는 세가지의 주요한 클래스 개념으로 나누어져 있었습니다. 그러나 네트워크 체계가 이러한 3가지 분류로 모두 잘 들어맞는 것이 아니어서 최대 254대의 호스트를 수용할 수 있는 C클래스를 여러 개 써야 하지만 그렇다고 65534대의 호스트를 수용하는 B클래스를 사용하기에는 불충분한 규모의 기관들이 과거에 B클래스를 할당받게 되어 IP주소는 매우 빠르게 소진되어갔습니다. 이러한 문제를 해결하기 위해 CIDR는 IP주소의 임의 개수의 연속적인 비트로 네트워크를 할당하게 되어, 어떤 기관에서 B클래스 규모보다 4배 정도 큰 주소 공간이 필요하다면 14비트를 이용해 네트워크를 나타내고 나머지 18비트의 공간을 (Bzmffotmdml 4배)을 사용하게 할 수 있습니다.

1.1.4 인버스 신청

인버스 도메인은 IP에 대해 해당 도메인을 역으로 찾을 수 있도록 하는 서비스입니다.
보통 ISP(Internet Service Provider)에서 IP를 할당받을 때 같이 신청합니다.
다음과 같이 인버스 도메인에 대한 네임서버가 in-addr.arpa 네임스페이스에 등록되어 있는지 확인합니다.

$ nslookup -type=ns 1.1.200.in-addr.arpa (C Class 200.1.1.x를 할당 받았을 경우)

멘트: 실무에서 인버스(리버스)가 사용되는경우
메일발송서버가 인버스등록이 안되어 있는경우, 상대 메일서버에서 스팸으로 간주되어 메일을 삭제하기도한다.

- 등록법은 KT 기업고객인경우 http://dns.kornet.net 고객문의에 신청한다.
- KT이외의 ISP인경우는 각 ISP는 DNS담당자에게 문의하면 된다.
- 메일 서버에서 확인시 사용되는부분이므로, 개인은 인버스 신청을 할필요가 없다.

짧은시간에 이해하시려면 교육을 들으시면 됩니다.^^
[DNS교육] DNS 장애처리 및 보안설정 신청 : http://www.bpan.com/edu_new/edu_lec/49

1.1 DNS서버의 Master File Format

2011.04.10 19:01

가이드: 아래부분은 설정형식입니다. 그냥 한번보고 넘어가시면됩니다. 찐한 색만 잘 보세요 ^^

1.1 DNS서버의 Master File Format

1.1.1 리소스 레코드 문법

파일들의 형식은 항목들의 연속입니다. 항목들은 라인 단위로 이루어져있으나, 괄호를 이용하면 여러 라인에 결쳐 항목들을 계속 나열할 수 가 있습니다. 텍스트 글자는 Ctrl 를 텍스트에 가질 수 있습니다. 탭이나 공백들은 항목을 구분하는 구분자 기능을 합니다. 마스터 파일의 각 라인은 주석문으로 끝날 수 있고, 주석문은 세미콜론 (';')으로 시작합니다.

Blank [comment]
공백 라인은 파일 내의 어느 곳에 있어도 됩니다.

$ORIGIN domain-name [comment]
$ORIGIN 뒤에는 도메인 네임이 오며, 현재의 기원을 변경합니다.

$INCLUDE file-name [domain-name] [comment]
$INCLUDE 는 지정한 파일을 현재 파일에 삽입하고, 포함되는 파일에 대한 기원을 바꾸는 도메인 네임을 설정할 수 있으나 부모 파일의 기원을 변경하는 것은 아닙니다.

domain-namerr [comment]
blankrr [comment]

위의 두 형식은 RR(리소스레코드)를 나타냅니다. RR에 대한 항목이 공백으로 시작하면, 그 RR은 바로 직전에 언급된 도메인에 속하는 것이고, 도메인 네임으로 시작하면 소유주가 그 도메인 네임이 됩니다.

리소스 레코드 형식
[TTL] [class] type RDATA
[class] [TTL] type RDATA

TTL과 class는 여러 가지 중에 선택할 수 있고, 종류에 따라 적합한 RDATA 값이 옵니다.
종류는 표준 약어를 이용하고 TTL은 십진수 정수입니다. 도메인 네임의 레이블들은 문자열로 나타내어지고 점으로 구분됩니다. 임의의 문자들을 도메인 네임 내에 저장하려면 quoting(따옴표로 묶거나 백슬래시를 앞에 붙이는 기법)을 이용합니다.

. 루트
@ 나 홀로 @문자는 현재의 기원을 나타내는데 이용
₩X X가 숫자(0-9) 외의 문자이면 그 문자의 특수한 의미 없이 문자 자체를 적어주기 위함
₩DDD 각 D가 숫자인 경우, DDD가 나타내는 십진수에 해당하는 옥텟을 뜻하고 이 옥텟은 텍스트로 간주함.
( ) 괄호는 여러 라인에 걸쳐 데이터를 묶어주기 위해 이용. 괄호 내에서는 라인 끝 문자들이 인식되지 않음
; 세미콜론은 주석문 시작을 알림. 라인의 뒷부분은 모두 무시됨.

대소문자 DNS에 이용되는 모든 문자열들은 대소문자를 구별하지 않음.

1.1.2 A, PTR, NS, MX, SRV, CNAME, SOA 레코더

A Address 이름을 주소로 맵핑
```
localhost.movie.edu.    IN    A    127.0.0.1
```

PTR Pointer 주소를 이름으로 맵핑
```
1.249.249.192.in-addr.arpa.    IN    PTR    wormhole.movie.edu.
```

NS Name Server 본 영역에 대한 네임 서버 나열
```
movie.edu.    IN    NS    terminator.movie.edu
```

MX Mail eXchange 메일 익스체인지
```
ora.com.    IN    MX    0     ora.ora.com.
            IN    MX    10    ruby.ora.com.
```

CNAME canonical name 전형적인(canonical) 이름 (별명을 위한 것)
```
wh.movie.edu.  IN  CNAME  wormhole.movie.edu.
```

SOA start of authority 본 영역에 대한 권한(authority)을 나타냄

```
movie.edu.    IN    SOA    terminator.movie.edu.    al.robocop.movie.edu. (
1                 ; 시리얼 번호
10800             ; 3시간 후에 리프레시
3600              ; 1시간 후에 재시도
604800            ; 1주일 후에 만료
86400 ) ; 최소 하루의 TTL
```

HINFO Host Information
호스트 기본 정보 (CPU, OS ..)
```
grizzly.movie.edu.    IN    HINFO    SPARC10    Solaris
```

1.1.3 축약어

도메인 네임 자동 확장
환경설정 파일의 도메인 네임은 영역 데이터 파일 내의 모든 데이터의 기원(origin)입니다.

점(.)으로 끝나지 않은 호스트뒤에는 자동으로 도메인이 붙게 됩니다.
따라서 아래 둘은 같은 설정입니다.

```
        Robocop.movie.edu.      IN      A       192.249.249.2
->      robocop                 IN      A       192.249.249.2

        2.249.249.192.in-addr.arpa.     IN      PTR     Robocop.movie.edu.
->      2                               IN      PTR     Robocop.movie.edu.
```

```
        Robocop.movie.edu       IN      A       192.249.249.2
```

@ 기호
도메인 네임이 기원과 같다면 도메인 네임을 '@' 로 나타낼수 있으며 SOA 레코드에서 많이 볼수 있습니다.

마지막 이름 반복

라인의 첫째 열 이름이 공백문자이거나 탭문자이면, 가장 최근의 리소스 레코드의 이름을 이용합니다.

```
        www             IN      A       200.1.1.2
                        IN      A       200.1.1.3
```

두번째 레코드에는 wormhole이라는 이름이 내포되어 있습니다.
따라서 www 의 ip 는 200.1.1.2 와 200.1.1.3 이 됩니다.

RR 레코드의 종류가 다르더라도 적용할 수 있습니다.

짧은시간에 이해하시려면 교육을 들으시면 됩니다.^^
[DNS교육] DNS 장애처리 및 보안설정 신청 : http://www.bpan.com/edu_new/edu_lec/49

1.1 DNS네임서버 Named.conf 의 문법

2011.04.10 19:03

Named.conf의 문법입니다.
서버에서 DNS데몬 시작시 제일 먼저 읽는 파일입니다.

BIND8을 기준으로 작성되어 옵션들이 많습니다. 그냥 쭉 함보세요 ^^

1.1 Named.conf 의 문법

```
options {
    directory "/var/named";
     named-xfer "/usr/libexec/named-xfer";    // _PATH_XFER
     dump-file "named_dump.db";   // _PATH_DUMPFILE
     pid-file "/var/run/named.pid";  // _PATH_PIDFILE
     statistics-file "named.stats";  // _PATH_STATS
     memstatistics-file "named.memstats";     // _PATH_MEMSTATS
     check-names master fail;       ; <- 언더바 사용시 문법체크를 안하게 해주는 설정
     check-names slave warn;        ;<- 언더바 사용시 문법체크를 안하게 해주는 설정
     check-names response ignore;   ;<- 언더바 사용시 문법체크를 안하게 해주는 설정
     host-statistics no;
     deallocate-on-exit no;       // Painstakingly deallocate all
                     // objects when exiting instead of
                     // letting the OS clean up for us.
                     // Useful a memory leak is suspected.
                     // Final statistics are written to the
                     // memstatistics-file.
     datasize default;
     stacksize default;
     coresize default;
     files unlimited;
     recursion yes;
     fetch-glue yes;
     fake-iquery no;
     notify yes;          // send NOTIFY messages.  You can set
                     // notify on a zone-by-zone
                     // basis in the "zone" statement
                     // see (below)
```

```
    // notify explicit;         // only sent the notifies to the
                    // also-notify list
    serial-queries 4;       // number of parallel SOA queries
                    // we can have outstanding for master
                    // zone change testing purposes
    auth-nxdomain yes;          // always set AA on NXDOMAIN.
                    // don't set this to 'no' unless
                    // you know what you're doing -- older
                    // servers won't like it.
    multiple-cnames no;         // if yes, then a name my have more
                    // than one CNAME RR.  This use
                    // is non-standard and is not
                    // recommended, but it is available
                    // because previous releases supported
                    // it and it was used by large sites
                    // for load balancing.
    allow-query { any; };  // 보안상 권장하지 않음.
    allow-transfer { any; };   // 보안상 권장하지 않음.
    transfers-in 10;        // DEFAULT_XFERS_RUNNING, cannot be
                    // set > than MAX_XFERS_RUNNING (20)
    transfers-per-ns 2;         // DEFAULT_XFERS_PER_NS
    transfers-out 0;        // not implemented
    max-transfer-time-in 120;     // MAX_XFER_TIME; the default number
                    // of minutes an inbound zone transfer
                    // may run.  May be set on a per-zone
                    // basis.
    transfer-format one-answer;
    query-source address * port *;      // for IPv4 query
    query-source-v6 address * port *;   // for IPv6 query*
    forward first;
    forwarders { };             // default is no forwarders
forwarders {
        168.126.63.1;
        168.126.63.2;
     };
    */
    topology { localhost; localnets; }; // prefer local nameservers
    /*
     * Here's a more complicated topology example; it's commented out
     * because only one topology block is allowed.
     *
    topology {
```

```
        10/8;            // prefer network 10.0.0.0
                         // netmask 255.0.0.0 most
        !1.2.3/24;       // don't like 1.2.3.0 netmask
                         // 255.255.255.0 at all
        { 1.2/16; 3/8; }; // like 1.2.0.0 netmask 255.255.0.0
                         // and 3.0.0.0 netmask 255.0.0.0
                         // equally well, but less than 10/8
    };
    */

    listen-on port 53 { any; };   // listen for queries on port 53 on
                         // any interface on the system
                         // (i.e. all interfaces).  The
                         // "port 53" is optional; if you
                         // don't specify a port, port 53
                         // is assumed.
listen-on { 5.6.7.8; };      // listen on port 53 on interface
                         // 5.6.7.8
    listen-on port 1234 {        // listen on port 1234 on any
        !1.2.3.4;        // interface on network 1.2.3
        1.2.3/24;        // netmask 255.255.255.0, except for
    };                   // interface 1.2.3.4.
    */

    /*
     * Interval Timers
     */
    cleaning-interval 60;        // clean the cache of expired RRs
                         // every 'cleaning-interval' minutes
    interface-interval 60;       // scan for new or deleted interfaces
                         // every 'interface-interval' minutes
    statistics-interval 60;      // log statistics every
                         // 'statistics-interval' minutes
    /*
     * IXFR options
    */
   maintain-ixfr-base no;   // If yes, keep transaction log file for IXFR
   max-ixfr-log-size 20;     // Not implemented, maximum size the
                         // IXFR transaction log file to grow
};
```

1.1.1 Working Directory (작업 디렉토리)

```
options {
        directory "/var/named";
 };
```

마스터 존파일, 슬레이브 존파일, 시스템 파일 (named.pid, named-xfer, named_dump.db, named.stats) 등이 생성되는 기본 위치를 의미합니다. 누구나 쓰기를 할 수 있는 권한이 있는(world-writable) 디렉토리는 피해야 합니다.

1.1.2 암호키 (cryptographic keys)

아직 국내에서는 TSIG를 거의 사용하지 않습니다.
보통 서버간의 Zone전송할때 키인증을 통해 보안강화로 사용됩니다.

// TSIG
BIND 8.2는 트랜잭션 서명(transaction signature)을 이용해 dns 메시지를 안전하게 하는 새로운 메커니즘을 소개하는데 이것을 간단히 TSIG라고 합니다.
TSIG는 공유하는 비밀값(Shared secret)과 단방향 해시(hash) 함수를 이용해 DNS메시지(특히 응답과 업데이트)를 인증합니다.
현재 RFC2845에 기술되어 있고, 네임 서버가 DNS 메시지의 additional section 에 TSIG 레코드를 추가합니다. 이 TSIG레코드는 DNS 메시지를 '서명' 하는 역할을 하고, 메시지 송신자와 수신자가 공유하는 암호키를 가지고 있어서, 그 메시지가 전송 도중에 변조되지 않았음을 입증합니다.

```
key sample_key {            // for TSIG
     algorithm hmac-md5;          // hmac-md5 is the supported algorithm
     secret "abcdefgh";           // base 64 encoded secret
};
key key2 {
     algorithm hmac-md5;
     secret "87654321";
};
```

1.1.3 주소 일치 리스트(Address Match Lists) 와 ACL

주소 일치 리스트는 IP주소를 하나 이상 지정하는 항목의 리스트입니다.
리스트의 요소는 개별적인 IP주소, IP접두사(예: 15/8; 192.168.1.192/26;), 또는
이름있는 엑세스 제어 리스트(acl "name" { address_match list; };)일 수 있습니다.

미리 정의된 네 개의 엑세스 리스트

none IP주소 없음
any 모든 IP주소
localhost 로컬호스트의 IP주소 (예를들어 네임 서버에서 실행된것 중 하나)
localnets 로컬호스트의 인터페이스가 속한 네트워크

엑세스 리스트 예

```
acl "HP-NET" {
    { 15/8; };
};

acl "internal" {
    203.255.1.1.192/26; };
};
```

명명된 주소 일치 리스트를 이용하면 타이핑하는 수고를 덜 수 있을 뿐만 아니라 named.conf 파일을 훨씬 이해하기 쉽게 작성할 수 있습니다.

1.1.4 ndc와 controls (BIND8)

Bind 8.2부터 특수 제어 채널로 메시지를 보냄으로써 네임 서버를 제어하는 방법이 생겼습니다.
이 제어 채널은 유닉스 도메인 소켓이거나 메시지를 청취할 TCP 포트입니다. 제한된 개수의 시그널에 비해 제어 채널은 매우 유연하고, 이것을 통해 네임 서버에 메시지를 날리는 것이 ndc 프로그램입니다.
Ndc를 인자없이 실행하면 ndc는 /var/run/ndc라는 유닉스 도메인 소캣을 통해 로컬 호스트에서 돌고 있는 네임 서버와 대화합니다. **이 소켓은 루트의 소유이고, 소유자만 읽고 쓰는 것이 가능합니다.**
소켓의 경로명이나 허가는 controls 구문을 이용해 바꿀 수 있습니다.

예)

```
controls {
        unix /etc/ndc   perm 0660  owner 0 group 53;
};
```

ndc는 TCP 소켓을 통해 로컬이 아닌 원격 호스트의 네임 서버에게 메시지를 보낼수 있습니다.

```
# ndc □c 127.0.0.1/953
```

네임서버가 특정한 TCP포트를 통해 제어 메시지를 기다리도록 설정할 수 있다.

```
Controls {
        Inet 127.0.0.1 port 953  allow { localhost; };
```

};

비대화식 모드 : 명령행에 지정하는 방식. 그냥실행하는 것으로 보통 이 방법을 사용한다.
네임서버에 부하를 주지않고 변경된 설정을 다시 읽는다.
 # ndc reload (bind8)

대화식 모드
ndc
Type help □or- /h if you need help.
ndc〉 help
(builtin) start - start the server
(builtin) restart - stop server if any, start a new one
getpid
status
stop
exec
reload [zone] ...
reconfig [-noexpired] (just sees new/gone zones)
dumpdb
stats [clear]
trace [level]
notrace
querylog
qrylog
help
quit
args

종료
ndc〉/e

1.1.5 rndc와 controls (BIND9)

BIND 8처럼 controls 구문을 이용해 네임 서버가 제어 메시지를 받아들이는 방법을 제어하는데 문법은 같지만 inet 서브 구문이 허용된다는 점이 다릅니다. 제어 채널을 위한 유닉스 도메인 소켓은 지원하지 않습니다.
포트는 지정하지 않을 수 있고, **기본적으로 포트 953을 청취(listen)합니다.** Rndc 사용자들이 자신을 인증하기 위한 암호키가 필요합니다.

```
Controls {
        Inet * allow { any; } keys {  “rndc-key”  ; };
};
```

keys 서브 구문에 지정한 키의 실제 값은 다음처럼 key 구문에서 정의합니다.

```
Key  “rndc-key”  {
        Algorithm hmac-md5;
        Secre  “Zm9vCg==” ;
};
```

현재는 HMAC-MD5 알고리즘만 지원되고 빠른 MD5 보안 해시 알고리즘을 이용해 인증을 수행합니다. 비밀값을 생성하려면 mmencode 나 dnssec-keygen을 이용하면 됩니다.

Rndc를 이용하려면 rndc.conf 파일을 생성함으로써 rndc에게 어떤 인증키를 이용할 것인지 그리고 어떤 네임 서버가 그 키를 이용할 것인지를 알려주어야 합니다.
Rndc.conf 파일 속의 키의 이름과 비밀값은 반드시 named.conf 속의 키 정의와 일치해야 합니다.

rndc가 안되면 rndc.conf를 만들고, named.conf를 수정해야 합니다. http://cafe.naver.com/dnspro/1405

짧은시간에 이해하시려면 교육을 들으시면 됩니다.^^
[DNS교육] DNS 장애처리 및 보안설정 신청 : http://www.bpan.com/edu_new/edu_lec/49

1.1 DNS Zones File

2011.04.10 19:05

1.1 DNS Zones File

1.1.1 Hint 파일

로컬 정보 이외에도 네임 서버는 루트 도메인에 대한 네임 서버들이 어디에 있는지 알아야 합니다.
이 정보는 인터넷 호스트 ftp.rs.internic.net (198.41.0.6)에서 가져올 수 있습니다. 익명 ftp 서비스를 이용하여 domain이라는 서브 디렉토리에 있는 named.root 파일을 가져와 이용하면 됩니다.

도메인 네임 '.' 은 루트 영역을 의미하고, 루트 영역의 네임 서버는 언제라도 바뀔 수가 있으므로 최신으로 갱신할 필요가 있습니다.
네임 서버는 named.root 파일의 데이터를 루트 힌트라 하여 메모리의 특별한 위치에 보관하며 폐기하지 않습니다.
힌트 데이터를 이용하여 루트 네임 서버들에게 최신 목록을 질의하여 그 목록을 캐싱합니다.

1.1.2 Master Zone설정

예) serverchk.com.zone 파일

```
$TTL 10M
@          IN        SOA       ns1.serverchk.com.      al.serverchk.com.edu. (

        2010102001        ; 시리얼번호, 10자리까지 가능하며, Slave서버가 이 숫자를 비교하여 전송받는다.
        3h                ; 3시간 후에 리프레시, Slave 서버가 3시간마다 정보요청시도함
        1h                ; 1시간 후에 재시도 , Slave 서버가 전송요청실폐시 1시간마다 정보요청시도함
        1w                ; 1주일 후에 만료 , Slave서버가 가져간 정보가 1주일동안만 보관한다.
        1h )              ; 1시간의 부정적 캐싱 TTL , 없는 도메인에 대한 정보를 캐싱하는 시간

            IN        NS        ns1.serverchk.com.
            IN        NS        ns2.serverchk.com.

localhost       IN        A         127.0.0.1
ns1             IN        A         200.1.1.1
ns2             IN        A         210.2.2.1
www             IN        A         200.1.1.100
```

// SOA에 ns1.serverchk.com. 는 Master 네임서버를 적어주어야한다.
notify시 NS레코더중 Master 네임서버 레코더를 제외하고, Slave에 notify가 보내지는데 이 부분을 참고해(SOA에 NS레코더로 지정된이름을 제외한) 다른 NS레코더로 지정된 서버(Slave)에 notify가 보내진다.

notify란, Maser NS의 정보가 변경될시, 다른 네임서버(NS)에 정보가 변경되었다고 알려주는 것인다.

1.1.4 Reverse Zone설정 (리버스,인버스 설정)

; ISP네임서버 요청하여 설정하는 부분이며, 메일서버 ip에 대해서는 리버스 설정을 하여야 많은 해외메일 서버들은 수신을 할수 있다.

예) db.192.24.249

```
$TTL 10M
 @          IN          SOA       terminator.movie.edu.      al.robocop.movie.edu. (
                        2                  ; 시리얼번호
                       3h   ; 3시간 후에 리프레시
                       1h   ; 1시간 후에 재시도
                       1w   ; 1주일 후에 만료
                       1h )             ; 1시간의 부정적 캐싱 TTL

          IN          NS        terminator.movie.edu.
          IN          NS        wormhole.movie.edu.
1         IN          PTR       wormhole.movie.edu.
2         IN          PTR       Robocop.movie.edu.
3         IN          PTR       terminator.movie.edu.
```

짧은시간에 이해하시려면 교육을 들으시면 됩니다.^^
[DNS교육] DNS 장애처리 및 보안설정 신청 : http://www.bpan.com/edu_new/edu_lec/49

1.1 DNS Resolver 이론

2011.04.10 19:05

1.1 DNS Resolver 이론

리졸버는 DNS의 클라이언트이며 호스트의 정보를 구하는 프로그램의 요청을 네임 서버에 대한 질의 형태로 번역하고, 그 질의에 대한 응답을 프로그램에 적절한 형태로 변경하는 일이 리졸버의 역할입니다. 대부분의 리졸버 설정은 /etc/resolv.conf 파일에서 이루어집니다.
Domain 지시자, search 지시자 , nameserver 지시자, sortlist 지시자, 그리고 options 라는
다섯 개의 지시자를 resolv.conf 파일에서 이용할 수 있습니다.

1.1.1 로컬도메인네임(domain)

로컬 도메인 네임은 해당 호스트가 속한 도메인 네임으로, 대부분 리졸버가 돌고 있는 호스트의 영역을 나타내는 도메인 네임입니다. 예를 들어 호스트 terminator.movie.edu의 리졸버는 movie.edu 를 로컬도메인네임으로 이용할 것입니다.
리졸버는 로컬 호스트 네임을 이용해 이름을 해석합니다. 일반적으로 로컬 도메인 네임은 호스트 네임에서 첫번째” .” 이후의 도메인 네임을 말합니다.

또한 resolv.conf 파일에서 domain 지시자를 이용해 로컬 도메인 네임을 설정할 수도 있습니다.
domain 지시자로 로컬 도메인 네임을 설정했다면, 호스트 네임을 보고 로컬 도메인 네임을 결정하는 것이 아니라 resolv.conf 파일에 있는 domain 지시자에 설정된 값을 로컬 도메인 네임으로 가지게 됩니다.

키워드 domain을 라인의 첫번째 열에 쓰고 계속해서 공백문자, 로컬 도메인 네임 순으로 입력하고, 맨 마지막에 “.” 이 없어야 합니다.
Domain colospgs.co.us

1.1.2 Search 리스트

로컬 도메인 네임은 기본 search 리스트를 결정하고, 사용자가 FQDN 형태로 호스트 네임을 입력하지 않아도 되게 하며, FQDN 형태로 기술하지 않은 호스트 네임은 **search 리스트에 있는 도메인 네임을 하나씩 차례로 붙여 적절한 FQDN으로 만듭니다.**
예를 들어 **대부분의 유닉스 네트워크 명령어 telnet, ftp, rlogin, rsh 등은 search 리스트를 적용합니다.**

1.1.3 Name server 지시자

호스트에 네임 서버를 운영하고 싶지는 않지만 DNS를 이용하고 싶다면 nameserver 지시자를 사용합니다.
이것은 질의할 네임 서버의 주소를 리졸버에게 알려주어 해당 네임서버를 사용할 수 있도록 합니다.

Nameserver 168.126.63.1

로컬 호스트에 있는 네임 서버를 사용하려면 nameserver 지시자에 로컬 호스트의 IP주소나 제로 주소 0.0.0.0을 설정합니다.
대부분의 TCP/IP 기반에서 0.0.0.0은 자기 자신, 즉 로컬 호스트를 의미합니다.
제로 주소 0.0.0.0을 이해하지 못하는 호스트라면 루프백 주소 127.0.0.1을 사용합니다.

Nameserver 지시자를 사용해 최대 3개까지의 네임 서버를 지정할 수 있고 나열된 순서대로 네임 서버를 사용합니다.

1.1.4 BIND Resolver 설정 예제

로컬 네임 서버가 없는 경우 resolv.conf 예

```
search movie.edu pixar.com
nameserver 192.249.249.1
nameserver 192.249.249.3
```

로컬네임서버가 있는 경우 resolv.conf 예

```
domain movie.edu
nameserver 0.0.0.0
nameserver 192.249.249.3
nameserver 192.249.249.1
options timeout:2   〈- 1차 네임서버 응답안될시 2초후 두번째시도. 기본값 5초, 최대 30초
```

1.1.5 서비스 동작의 차이

telnet , ftp, rlogin, rsh 같은 프로그램은 입력한 도메인 네임이 '.' 으로 끝나지 않으면 search 리스트를 적용합니다.
만약 movie.edu가 있다면 다음과 같은 형태로 입력할 수 있습니다.

```
%telnet misery 또는
%telnet misery.movie.edu 또는
%telnet misery.movie.edu.
```

세가지 모두 동일한 호스트에 접속할 것이며, 다른 서비스에서도 리졸버는 동일하게 동작합니다.
주소를 찾을 때 네임 서버가 여러 개의 IP주소를 전해줄 수 있는데, 최근 버전의 telnet, ftp, 웹브라우져 등은 첫번째로 받은 IP주소로 연결

을 시도하고 이것이 실패할 경우 다음 IP주소로 재시도 하게 됩니다.

1.1.6 윈도우 NT4.0 리졸버 환경설정

윈도우 NT에서는 LAN 리졸버 설정이 윈도우 95와 유사한 인터페이스에서 이루어집니다.
DNS를 설정하려면 제어판-〉 네트워크-〉 프로토콜을 실행하고 TCP/IP 프로토콜을 더블 클릭한 후 DNS탭을 선택하면 됩니다. 윈도우 NT4.0 리졸버는 각각의 이름 -〉 주소 변환 결과를 캐시하고 캐시되는 시간은 결과 레코드에 지정되는 생존값을 다릅니다.

서비스팩4리졸버는 새로운 재전송 알고리즘을 채택하여, 찾을 DNS 서버 목록의 첫 네임 서버에게 첫 질의를 전송하고 1초를 기다린 후 응답이 없으면 질의를 다시 재전송합니다. 이제는 정적 설정, DHCP, RAS 등을 통해 자신이 이미 알고 있는 모든 네임 서버에게 다시 보냅니다. 만일 어떤 네임 서버도 2초 이내에 응답하지 않으면 리졸버는 네임 서버 모두에게 다시 재전송합니다. 재전송을 다시 할때마다 시간제한은 계속 2배로 늘어나고, 총 4번의 재전송을 하게 되며 15초가 소용됩니다. (Q19855) 이런 재전송 방법은 모든 네임 서버에게 다소 높은 부하를 줄수 있으므로 리졸버의 찾을 DNS 목록에서 제일 첫 서버가 충분히 빠른 장비어야 하며, 서버 목록을 최소로 유지해 불필요한 설정을 피해야 합니다.

1.1.7 윈도우 2000 리졸버 환경설정

시작을 누르고 설정을 선택한 후 네트워크 및 전화접속 연결을 선택합니다. 로컬 영역 연결 아이콘을 마우스로 오른쪽 클릭한 후 등록정보를 선택합니다.
인터넷 프로토콜(TCP/IP)를 더블 클릭하면 리졸버 환경설정 창이 뜹니다. DNS 서버 주소 받기 버튼을 자동으로 선택하면 로컬 DHCP 서버로부터 네임 서버에 대한 정보를 얻어와 그 네임 서버를 이용합니다. 다음 DNS 서버 주소 사용버튼을 선택하면 기본 설정 DNS 서버 및 보조 DNS 서버 항목에 적어놓은 네임 서버로 질의를 보냅니다. 리졸버 고급 환경설정을 하려면 고급 버튼을 누르고 DNS 탭을 선택합니다., 이전의 기본 환경 설정 창에 지정했던 네임 서버들의 주소가 DNS 서버주소 항목에 나열되어 있을 것입니다.

윈도우 2000 리졸버는 윈도우 NT 4.0 서비스팩4의 리 졸버와 동일한 재전송 알고리즘을 이용해 나열된 네임 서버 모두에게 질의를 재전송합니다. 서로 다른 두 네임 서버로부터 상이한 대답을 각각 얻었다면 윈도우 2000 리졸버는 부정적인 응답(그런 도메인 네임 없음 또는 그런 데이터 없음)을 일단 무시합니다. 각 인터페이스에 대해 설정된 네임 서버로부터 부정적인 응답을 얻은 경우에만 부정적인 응답을 반환하고 긍정적인 대답을 하나라도 얻으면 그 긍정적인 대답을 반환합니다.

주 DNS 도메인 및 연결 특정 DNS 접미사 추가 버튼을 선택하면 리졸버가 주 DNS 접미사 및 연결 특정적인 DNS 접미사를 search 리스트처럼 이용합니다. 하단의 DNS에 이 연결의 주소를 등록을 선택하면 동적 업데이트 메커니즘을 이용해 자신의 이름과 주소로 이루어진 주소 레코드를 추가하려고 시도합니다.

DNS 등록에 이 연결의 DNS 접미사 사용을 선택하면 동적업데이트 시도시 이 연결에 특정적인 도메인 네임을 이용할 것인지 아니면 그 컴퓨터의 주 DNS 접미사를 이용하도록 할 것인지를 조절합니다. 이러한 자동 등록 기능은 WINS(Windows Internet Name Service)와 NetBIOS 네임 서비스의 종말을 고하는 것이라고 할 수 있습니다.

짧은시간에 이해하시려면 교육을 들으시면 됩니다.^^

[DNS교육] DNS 장애처리 및 보안설정 신청 : http://www.bpan.com/edu_new/edu_lec/49

1.1 DNS 기본보안

2011.04.10 19:07

1.1 DNS 기본보안 설정

1.1.1 버전 숨기기

BIND 4.9 이후부터는 특정 형태의 질의를 수신하면 자신의 버전 정보를 응답하는 기능이 있습니다.

로컬 버전정보탐색법

```
# dig txt chaos version.bind.
```

외부에서 버전정보탐색법

```
# dig @168.126.63.1 txt chaos version.bind.
```

// BIND 8.2와 그 이후 버전에서는 설정으로 이런 정보 유출을 막을 수 있습니다.

버전 정보 숨기기

```
#vi /etc/named.conf
options {
        version "No! Touch!!!";
};
```

1.1.2 단일 장애 지점 (Single points of Failure) 피하기

http://www.menandmice.com/2000/2110_single_point.html

대부분의 도메인 레지스트라에서는 도메인 등록시 네임 서버를 2개 이상 등록해야만 하는데
만약 1대의 네임서버만을 운영하다가 해당 네트워크가 다운이 되면, 업무상 많은 손실이 발생할 수 있기 때문으로 항상 도메인 서비스가 끊기지 않도록 사전 예방해야 합니다.

Single point of failure 에 노출되었는지 확인하는 방법

1) 도메인 서비스를 위한 네임서버가 1대인 경우
2) 도메인 서비스를 위한 네임서버들 중에 1대에만 존설정한 경우
3) 도메인 서비스를 위한 네임서버들이 모두 존설정을 했지만 물리적으로 같은 subnet에 위치하거나 같은 장소에 위치하거나 어떤 특정한 장비에 의존해 있는 경우

해결책)

1) 도메인 서비스용 DNS 서버를 2개이상 보유하기
2) 도메인에 대한 설정이 해당 DNS 서버들 모두에게 설정되도록 하기
3) 물리적으로 분리하기

1.1.3 트래픽 필터링

TCP/IP상에서 IP주소 Port 번호 등을 기반으로 한 packet filtering 가능
네임서버기능만 하는 호스트라면, 해당 서버들에 불필요한 트래픽이 가지 않도록 필터링합니다.
즉 인터넷에서 UDP와 TCP포트 53번 외의 트래픽을 차단합니다.

어떤 네트워크는 네트워크의 연결이 패킷 단위로 요금이 책정되거나 회선의 속도가 매우 느려 다량의 트래픽을 사이트 외부로 전송하는데 곤란을 겪는 경우가 있다. 이런 상황에서는 사이트 바깥으로 나가는 DNS 트래픽을 가장 최소로 제한할 필요가 있는데
BIND가 포워더(forwarders)라는 메커니즘을 이용해 이런 역할 해줍니다.

특정 네임 서버에 도메인 네임 탐색 업무를 몰아주려면 포워더(forwarder)를 이용하는게 유용합니다. 예를 들어 네트워크에서 호스트 하나만 인터넷에 연결되어 있고 그 호스트에서 네임 서버가 돌고 있다면, 그 서버를 포워더로 이용하도록 다른 네임 서버를 설정해 모든 서버가 도메인 네임을 탐색하게 할 수 있습니다.

```
Options {
        Forwarders { 192.249.249.1; 192.249.249.3; };
};
```

1.1.4 Recursive 쿼리 제한

BIND 8과 9의 allow-query 서브 구문에서 질의에 대한 IP주소 기반의 액세스 리스트를 만들 있습니다. 이 액세스 리스트를 늑정 영역에 적용하거나 네임 서버가 수신하는 모든 질의에 적용할 수 있습니다.

1) 모든 질의 제한
allow-query 서브 구문의 형식

```
options {
        allow-query { address_match_list; };
};
```

2) 특정 영역의 질의 제한
액세스 제어 리스트(ACL)를 특정 영역에 적용할 수도 있습니다. 이런 경우에는 보호하려는 영역에 대한 zone 구문에 allow-query 서브 구문을 이용합니다.

```
Acl "HP-NET" { 15/8; };
Zone "hp.com" {
        Type slave;
        File "bak.hp.com";
        Masters { 15.255.152.2; };
};
```

1.1.5 서버정보 보호 Zone Transfer 제한 설정법

전체도메인에 대해 영역 전송 제한 및 허용법
네임서버에서만 서버정보를 전송해갈수 있도록 설정 한다.

1) BIND 8 9 allow-transfer 설정법

```
# vi /etc/named.conf

options {
        allow-transfer { 127.0.0.1; 200.1.1.1; 200.2.2.2; };
};
// 설명: 200.1.1.1, 200.2.2.2 대신 실제 네임서버 IP를 적어주어야한다.
```

2) BIND 4.9 xfrnets 지시자 이용

```
Xfrnets 15.0.0.0 128.32.0.0

Zone "movie.edu" {
        Type master;
        File "db.movie.edu";
        Allow-transfer { 192.249.249.1; 192.253.253.9; };
};
```

기본적으로 모든 IP주소에 대해 영역 전송을 허용하기 때문에, 해커들이 슬레이브 서버로부터 영역을 쉽게 긁어갈 수 있다. 해당 서버가 Slave 네임서버로만 사용되면 아래와 같이 Zone 전송이 되지 않도록 설정한다.

```
# vi /etc/named.conf
options {
        allow-transfer { none ; };
```

};

또는 도메인에 따라 Master , Slave로 같이 운영중일때는 해당 Slave네임서버에서 Zone전송을 제약한다.

```
Zone “movie.edu” {
        Type slave;
        Masters { 200.1.1.1; };
        File “muisc.serverchk.com” ;
        Allow-transfer { none; };
};
```

짧은시간에 이해하시려면 교육을 들으시면 됩니다.^^
[DNS교육] DNS 장애처리 및 보안설정 신청 : http://www.bpan.com/edu_new/edu_lec/49

1.1 DNS 위협

2011.04.10 19:08

1.1 DNS 위협

1.1.1 스푸핑(Spoofing) : 가짜 데이터로 속이는 공격

스푸핑의 목적은 DNS 서버가 잘못된 응답을 하도록 만드는 것입니다.
이 방법은 공격자가 재귀질의를 특정 DNS 서버에 보내는데 DNS서버는 질의에 대해 이름분해를 합니다.
질의에 대한 답이 공격자가 통제하는 존입니다.
공격자의 네임서버에 의한 응답은 제3자가 해당 도메인에 대한 조작이 가능한 auth 레코드를 포함합니다. 그리고 그 auth 레코드는 잘못된 것입니다. 희생 서버는 가짜 레코드를 캐시합니다.

한번 스푸핑단한 리졸버는 캐쉬속에 있는 잘못된 레코드를 계속 사용하면서 이메일 사용 및 다른 인터넷 서비스를 틀리게 사용할 수 있습니다. 이것은 신용카드 정보, 무역관련 비밀정보 외에 민감한 정보의 보안 위협을 가져오게 됩니다.
Recent surveys indicate that 25-30% of servers on the Internet are spoofable. Further readings on DNS spoofing

1.1.2 DoS (Denial of Service)

http://www.cert.org/tech_tips/denial_of_service.html

유닉스의 루트 권한을 빼앗는 해킹만이 보안을 위협하는 공격이 아니면, 맘에 들지 않는 **서버가 정상적인 활동을 못하도록 만드는 것도 보안을 위협하는데 이것을 서비스 거부 공격이라고 합니다.**

1.1.3 BIND vulnerabilities

BIND 각 버전의 취약점

http://www.isc.org/products/BIND/

관리자는 취약점에 대한 정보를 늘 찾아봐야 하고 최신의 안전한 버전을 이용하도록 노력해야 합니다.
BIND는 버전별로 다른 형태의 공격이 있습니다. 해당 버전 정보를 입수한다면 그 버전에 적절한 공격이 가능할 것입니다.

짧은시간에 이해하시려면 교육을 들으시면 됩니다.^^

[DNS교육] DNS 장애처리 및 보안설정 신청 : http://www.bpan.com/edu_new/edu_lec/49

1.1 DNS 고급기능

2011.04.10 19:08

1.1 DNS 고급기능

1.1.1 동적 업데이트 (Dynamic Update) 이론과 구성

인터넷 세계는 점점 더 동적으로 되고 있습니다.
대부분의 기업이 DHCP를 사용해 IP주소를 동적으로 할당하고, ISP는 DHCP를 이용해 전화접속과 ADSL, 케이블 사용자에게 주소를 할당합니다. 이런 상황을 지원하기 위해 DNS 레코드를 동적으로 추가하거나 삭제하는 기능을 제공할 필요성으로 소개되었습니다. (RFC 2136)

BIND 8 9 은 동적 업데이트를 지원하고, 권한을 가진 업데이트자(authorized updater)가 역역의 NS 레코드를 추출함으로써 영역의 권한을 가진 네임 서버를 찾아 리소스 레코드를 추가하고 삭제합니다. 명령행 프로그램인 nsupdate를 이용해 업데이틀 메시지를 수작업으로 만들 수 있습니다.

```
% nsupdate
Ø       prereq nxdomain mib.x.movie.edu.
Ø       update add mib.fx.movie.edu. 300 A 192.253.253.16
Ø
```

이 명령어는 mib.fx.movie.edu의 주소를 그 도메인 네임이 존재하지 않을 때만 추가하도록 서버에 지시합니다.
마지막 공백 라인은 nsupdate에 알리는 신호로 업데이트를 전송하도록 합니다.
동적 업데이트는 SOA 레코드와 하나의 NS 레코드를 제외한 레코드를 모두 삭제할 수 있어도 한 영역 전체를 흔적없이 삭제하는 것은 불가능하며 새로운 영역을 추가할 수는 없다는 제약이 있습니다.

BIND 8은 영역의 시리얼 번호를 증가하는 일을 5분 또는 업데이트 100번 동안 연기할 수 있습니다.
BIND 9은 동적 업데이트가 진행될 때마다 시리얼 번호를 변경합니다.
동적 업데이트를 수신할 때마다 업데이트할 작은 레코드를 로그 파일에 추가합니다.

BIND 8 9은 기본적으로 갖는 영역에 대한 동적 업데이트를 허용하지 않습니다.

예)

```
zone  "fx.movie.edu"  {
          type master;
          file  "db.fx.movie.edu" ;
          allow-update { 192.253.253.100; };          //dhcp 서버만 업데이트 허용
};
```

1.1.2 NOTIFY 이론과 구성

BIND 슬레이브는 원래 마스터를 주기적으로 검사해 영역 전송의 필요 여부를 결정하는데 주기적으로 검사하는 기간을 리프레시(refresh) 시간이라 부릅니다. 이런 주기적인 검사 방법을 이용하면 슬레이브가 영역이 바뀌었음을 인지하고서 마스터 네임 서버에서 새로운 영역 데이터를 가져올 때까지 최대 리프레시 시간 만큼의 지연이 생기므로, 영역 데이터가 수시로 업데이트되는 환경이라면 적절하지 않습니다.
RFC 1996은 주 마스터 서버가 영역 데이터가 변경되었음을 슬레이브에 알리는 메커니즘을 제안하고,
BIND 8, 9가 이런 기능을 구현한 것은 DNS NOTIFY(영역 변경 알림)이라 부릅니다.

동작방식은 주마스터 네임서버가 영역의 시리얼 번호가 바뀌었음을 인지하면, 특별한 알림을 그 영역의 모든 슬레이브 서버에 전송합니다.
주마스터는 영역의 NS 레코드의 목록을 보고 로컬 호스트인 도메인 네임과 영역의 SOA레코드의 MNAME 필드에 나열된 네임서버를 가리키는 레코드를 취해 어떤 서버가 그 영역에 대한 슬레이브인지를 결정합니다.
(Master인 자신은 제외하고 노티를 보냅니다.)

변경 사항을 인지하는 시간은 주 마스터 네임 서버를 재시동하면 모든 슬레이브 서버에 영역들의 최신 시리얼 번호를 통보합니다. 동적 업데이트로 인해 영역의 시리얼 번호가 증가해도 통보합니다.
변경되었다고 알려준 영역의 SOA 레코드를 마스터 서버에 요청하여 시리얼 번호가 더 크면 슬레이브는 영역 전송을 합니다.
마이크로소프트 DNS 서버도 NOFITY를 지원합니다.

```
// BIND 8 9 에서는 DNS NOTIFY가 기본적으로 활성화되어 있습니다.
options {

};

zone  "fx.movie.edu"  {
          type master;
          file  "db.fx.movie.edu" ;
          notify no;
};

zone  "fx.movie.edu"  {
          type slave;
          file  "bak.fx.movie.edu" ;
          notify yes;
         also-notify { 15.255.152.4; };    <-  notify리스트에 포함시켜서 notify한다.
                                                NS레코더로 등록안된 Slave서버에 notify함.
};

options {
          allow-notify { 192.249.249.17; };
};
```

1.1.3 Incremental Zone Transfer 이론과 구성

증진적 영역 전송(IXFR, incremental zone transfer) 은 슬레이브 네임 서버가 현재 가지고 있는 영역의 버전을 마스터 네임 서버에게 알려 자신의 버전과 마스터 네임 서버가 가지고 있는 최신 버전 사이의 변화된 데이터만 요구합니다. 이것은 영역 전송의 크기와 소요 시간을 상당히 줄일 수 있습니다.

IXFR은 BIND 8.2.3 이전까지는 잘 동작하지 않으나 BIND 9 은 이 기능을 잘 구현하고 있습니다.
영역 데이터 파일을 전부 다시 읽은 BIND 주 마스터 네임 서버는 현재의 영역과 이전 영역의 차이점을 계산할 수 없다는 한계가 있습니다.
IXFR의 장점을 최대한 살리기 위해서는 동적 업데이트만 이용해 영역을 수정하고 영역 데이터를 임의로 편집하지 않는 것입니다. BIND8 에서 IXFR 로그 파일의 이름은 영역 데이터 파일의 이름 뒤에 .ixfr을 붙입니다.

다음페이지 http://cafe.naver.com/dnspro/442

1.1 DNS 와 Firewall

2011.04.10 19:09

이 페이지는 진하게 된부분만 읽고 넘어가세요 ^^

1.1 DNS 와 Firewall

1.1.1 Inside-Out

- 포워딩

DNS 트래픽이 방화벽을 양방향으로 자유롭게 통과할 수 잇는 위험한 상황에 대비하기 위해 대부분의 사이트가 인터넷과 'DNS를 논할 수 있는' 내부 호스트를 제한하고 있습니다.
애플리케이션 게이트웨이 방화벽이나 DNS 트래픽을 통과시키는 기능이 없는 방화벽에서 인터넷의 네임 서버와 통신할 수 있는 호스트는 베이스천 밖에 없습니다.

패킷필터링 방화벽 관리자는 내부 네임 서버 일부만 인터넷 네임 서버와 통신할 수 있도록 방화벽을 설정할 수 있습니다. 이런 내부 네임 서버는 대부분 네트워크 관리자가 직접 제어하는 네임 서버가 실행되는 호스트입니다. 인터넷의 네임 서버에 직접 질의할 수 없는 내부 네임 서버는 직접 질의할 수 있는 네임 서버 중 하나에 질의를 포워딩 할 수 있어야 합니다. 즉 질의를 받은 내부 네임 서버는 그 질의를 자체적으로 리졸빙할 수 없는 경우, 포워더 중 하나로 그 질의를 포워딩하고 그 질의를 받은 서버가 인터넷의 네임 서버를 이용해 그 이름을 리졸빙합니다.
-iterative resolution
-hybrid(복합적인) architecture

1.1.2 Outside-In

- visibility
- 분할 네임공간

내부에서 이용하는 영역 데이터와는 다른 영역 데이터를 인터넷에 두고 싶어하는 기관이 상당수 있습니다. 대개의 경우, 기관의 인터넷 방화벽으로 인해 내부 영역 데이터는 인터넷과 무관하게 됩니다. 방화벽은 외부에서 내부 호스트를 직접 엑세스할 수 없게 하며 내부의 비공인 IP주소를 기관이 할당 받은 외부 공인 IP주소로 변환할 수 있습니다. 따라서 관계없는 정보를 외부에 노출하지 말아야 하고 내부 주소를 이에 대응되는 외부 주소로 변경해야 합니다. 대부분의 기관에서는 일명 '분할네임공간(split namedspace)' 이라는 것을 직접 만드어 잉용하고 있는데 진짜 네임 공간은 내부에서만 이용할 수 있고 인터넷에는 고르고 변환하거나 다음은 '쉐도우 네임공간 (shadow namespace)' 만 보여줍니다.

1.1.3 Views

방화벽 환경에서 유용하게 사용할 수 있는 메커니즘으로 한 그룹의 호스트에게는 하나의 환경설정을 제공하고 동시에 또 다른 그룹의 호스트에게는 다른 환경설정을 제공할 수 있습니다.

내부 호스트와 인터넷의 호스트 양쪽에서 질의를 받는 호스트에서 네임 서버를 운영하고 있다면 이 기능이 아주 편리합니다. view 구문은 options 구문 뒤에 나와야 하지만 꼭 바로 뒤에 위치해야 하는 것은 아닙니다.

View 구문의 순서는 매우 중요합니다.
호스트는 자신의 IP주소와 일치하는 첫번째 뷰를 보기 때문에 모든 주소에 해당하는 외부(external) 뷰를 처음에 나열하면 내부(internal) 뷰는 차단이 됩니다. View 구문을 하나 설정하더라도 모든 zone 구문을 나타내야 합니다.

1.1.4 Multiple named processes

스레스사용하지 않으려면, BIND9 컴파일시 아래 옵션을 사용한다.
 # ./configure --disable-threads

it'll let your name server take advantage of any extra CPUs your computer may have stashed away. But you may find the consequent output of ps confusing:

```
% ps ax | grep named
6052 ?        S      0:00 /usr/local/sbin/named
6053 ?        S      0:00 /usr/local/sbin/named
6054 ?        S      0:00 /usr/local/sbin/named
6055 ?        S      0:00 /usr/local/sbin/named
6056 ?        S      0:00 /usr/local/sbin/named
6318 pts/0    S      0:00 grep named
```

짧은시간에 이해하시려면 교육을 들으시면 됩니다.^^
[DNS교육] DNS 장애처리 및 보안설정 신청 : http://www.bpan.com/edu_new/edu_lec/49

1.1.1 DNS 장애처리 툴

2011.04.10 19:11

1.1.1 DNS 장애처리 툴

 # nslookup

nslookup은 한번에 하나의 네임 서버와 이야기를 합니다. 이것이 nslookup 의 행동과 리졸버(PC)의 행동의 차이점입니다.
리졸버(PC)는 resolv.conf의 nameserver 항목을 이용합니다.

Nslookup 은 resolv.conf의 첫번째 네임 서버에 질의를 시도해 이 네임 서버를 포기할때까지 계속 재시도 한 다음, 다음 순서의 네임 서버에 질의를 시도 합니다. 일단 응답을 얻으면 그 네임 서버를 고정시키고 다른 서버로는 시도하지 않습니다.

Nslookup에는 리졸버가 하는 것과 동일한 search 리스트가 구현되어 있어서 로컬 도메인 네임과 모든 조상 도메인 네임을 적용하려고 합니다. 네임 서버에는 search 리스트가 구현되어 있지 않아서 네임 서버처럼 행동하려면 search 기능을 꺼놓아야 합니다. 디버깅을 할 때는 search 리스트 기능을 off하거나 탐색할 도메인 네임의 끝에 점을 추가합니다.

 # dig

dig은 Domain Information Groper를 줄인 말로서 BIND4, 8, 9 에 들어가 있습니다.
Dig 에는 대화식 모드가 없으며 질의에 필요한 모든 항목을 명령행에 지정합니다.

1) Dig 옵션

 # dig @168.126.63.1 www.serverchk.com

2) 리버스 확인하는 -x 옵션

 # dig □x 10.0.0.1
-p port
+norec : 재귀 기능을 이용하지 않음
+vc : TCP 기반의 질의를 전송하게 됨

// host

host 는 BIND 8 9에 들어가 있으며 위임 관계를 쉽게 검사할 수 있습니다.
Host를 이용해 잘못된 내용을 검사하는 방법을 배우고 싶다면 부모 영역의 네임 서버가 가진 자기 영역의 NS 레코드를 탐색하여 그 정보가 올바른지 살펴보는 것입니다.

% host □t ns fx.movie.edu ns.movie.edu

// dnswalk

Dnswalk는 Perl로 제작된 스크립트로써 존재하지 않는 호스트를 가르키는 MX, PTR이 없는 A, 잘못된 CNAME, 유효하지 않은 이름문자,

누락된 트레일링 도트, 불필요나 글루 레코드, Lame Delegation 등 Zone 데이터베이스의 다양한 오류를 찾아준다. 미처 발견치 못한 문제점을 진단하는데 도움이 될 것이다. Dnswalk의 최신 버젼은 다음 주소에서 얻을 수 있다.
http://www.cis.ohio-state.edu/~barr/dnswalk/

dnswalk -raFl freebsd.org.

Dnswalk는 검사를 수행하기 위해 해당 도메인을 Zone Transfer 한 후 내부적으로 Dig와 Resolver 루틴을 사용한다. Delegation된 도메인을 따라가며 검사를 행하기 때문에 거대 도메인을 관리한다면 한번쯤 사용해봄직 하다.
Dnswalk is a DNS debugger written in Perl by David Barr, from
Pennsylvania State University. You'll find the latest version at
ftp://ftp.pop.psu.edu/pub/src/dnswalk. With the software comes a small document where the author points some useful advice so it may be worth reading it.

1.1.2 장애처리 테크닉

nslookup 장애처리
- 올바른 데이터 탐색
- 서버에서 응답이 없음
- 네임 서버의 주소에 대한 PTR 데이터 없음
- 질의 거절
- resolv.conf의 첫번째 네임 서버가 응답 없음
- 탐색되는 것 찾기
- 지정되지 않은 에러

#named -xfer 사용법
영역 전송에 문제가 생겼을 때 named가 영역 전송을 할 때까지 기다릴 필요가 없어 유용합니다.
Named-xfer가 없다면 dig 을 이용해 영역을 전송해 올수 있습니다.

 # Dig @terminator.movie.edu movie.edu axfr

네임 서버의 내부 데이터베이스를 캐시 정보를 포함해 몽땅 덤프하는 것은 문제점을 추적하는데 도움이 될 수 있다.

 # Ndc dumpdb / Rndc dumpdb 명령을 날리면 named는 자신의 권한있는 데이터, 캐시 데이터, 힌트데이터를 named_dump.db 파일에 덤프합니다.

1.1.3 일반적인 오류들

- 시리얼 번호 증가시키는 것을 있었음
- 주마스터 서버에 시그널 보내는 것을 잊었음
- 슬레이브 서버가 영역 데이터를 로드하지 못함
- 데이터베이스 파일에 이름은 추가했으나 PTR 레코드를 추가하는 것을 잊었음
- 환경설정 파일이나 영역 데이터 파일의 문법 에러
- DNS 데이터베이스 파일명 끝의 점 누락
- 루트 힌트 데이터 누락
- 네트워크 연결 단절
- 서브도메인 위임 정보 누락
- 잘못된 서브 도메인 위임 정보
- resolv.conf 의 문법 에러
- 로컬 도메인 네임이 설정되어 있지 않음
- 예기치 않은 소스로부터의 응답
- BIND 서버에서 MS DNS로 이전
- BIND 4에서 BIND 9 으로 이전

다음페이지 http://cafe.naver.com/dnspro/444

짧은시간에 이해하시려면 교육을 들으시면 됩니다.^^
[DNS교육] DNS 장애처리 및 보안설정 신청 : http://www.bpan.com/edu_new/edu_lec/49

1.1 DNS 서버 유지보수

2011.04.10 19:11

1.1 DNS 서버 유지보수

1.1.2 통계 활용

네임 서버가 얼마나 바쁜지 보고 싶으면 네임 서버의 통계를 주기적으로 살펴봐야 합니다.
통계치에서 눈여겨 봐야 할 한 가지는 서버가 초당 얼마나 많은 질의를 받고 있는가 하는 점입니다.
ndc stats
% kill □ABRT ‘cat /var/run/named.pid’

만일 BIND 8 네임 서버가 각 IP주소별 통계 항목을 보여주지 않으면 options 구문 내의 host-statistics yes로 설정해 호스트별 통계를 뽑도록 할 수 있습니다.

1.1.3 DNS debuggin 툴

장애 처리에 좋은 툴로서 각 질의마다 내부적으로 일어나는 동작에 대한 보고서를 얻게 됩니다. 디버깅 레벨에 따라 출력되는 정보의 양의 정보가 차이가 나지만 대부분 어떤 이름이 왜 탐색되지 않는지 등의 문제는 레벨 1로도 충분합니다.
디버깅 정보는 누적적이기 때문에 레벨2의 출력은 레벨 1의 출력이 포함됩니다. 출력되는 데이터는 네임 서버 시작, 데이터베이스 업데이트, 질의 처리, 영역 관리 등 네 가지 범주로 분류됩니다.

BIND 9 디버깅 레벨
레벨 1 □ 90

BIND 8 9 을 이용할 때 . Print-severity 로깅 옵션을 on으로 활성화하면 디버깅 레벨과 디버깅 메시지를 함께 출력하도록 네임 서버를 설정할 수 있다

Named.run
/etc/named □d 1 &
ndc trace 3
ndc notrace

1.1.4 Log 분석

네임 서버 named가 내는 syslog 메시지는 여러 가지입니다.

Unix 의 로그 위치 # tail -f /var/adm/messages
Linux의 로그 위치 # tail -f /var/log/messages

다음은 로그내용에 따른 처리법입니다.

1) 로그내용:
/etc/named.conf:53: cannot redefine zone '' class 1

조치 =〉 named.conf 파일에 같은 zone을 두 번 이상 입력했기 때문에 나타나는 메시지입니다. 여기서는 53가 해당 라인이므로 찾아서 삭제하시기 바랍니다.

2) 로그내용:
unapproved AXFR from [132.174.12.141].60685 for "fs.dedip.oclc.org
조치 =〉 먼저 여기서 표시된 132.174.12.141번 IP가 slave name server인지 확인하시기 바랍니다. named.conf의 ACL(access control list)에서 zone transfer를 허용한 네임서버 이외의 서버일 경우에 zone transfer가 안 되기 때문에 나타나는 메시지입니다. allow-transfer 부분에서 slave name server의 IP를 추가하시기 바랍니다.

```
# vi named.conf
options {
allow-transfer {
210.103.175.1;
                };
};
```

3) 로그내용:
uninterpretable server (axfr) for 도메인
조치 =〉 named와 named-xfer 의 버전이 같은지 확인해 보시기 바랍니다. Bind 4에서 8으로 업그레이드할 때 종종 발생할 수 있는 로그로 두개의 버전이 상이하여 발생하는 문제입니다. 해당 도메인이 전송되지 않아 폐기될 수 있습니다.

4) 로그내용:
bad referral (state.il.us !〈 SOS.STATE.IL.US)
or
bad referral (state.il.us !〈 SOS.STATE.IL.US) from [1.2.3.4].53
조치 =〉 sos.state.il.us를 쿼리했는데 state.il.us 를 참고하도록 응답받았다.
Indicates that while querying the SOS.STATE.IL.US name servers, your name server was referred to the state.il.us name servers.
Since a referral should always point to name servers authoritative for descendant zones, this is an error.
The name server that sent the referral is probably misconfigured, and not authoritative for the zone delegated to it.

5) 로그내용:
check_hints: root NS list in hints for class 1 does not match root NS list
조치 =〉 디렉토리안에 있는 힌트파일 db.cache (named.root) 의 루트 정보와 네임 서버가 응답을 받은 현재 루트 정보가 일치하지 않는 경우에 발생하며 최신 루트 힌트 파일로 업데이트를 애주어야 하고
ftp://ftp.rs.internic.net/domain/named.root 여기서 최근 힌트파일 정보를 다운받을 수 있습니다.

6) 로그내용:
CNAME and other data (invalid)
조치 =〉 존 파일안에 CNAME 레코드와 다른 레코드(MX, SOA, NS등)과 연계해서 사용하지 않아야 하고 이런 경우 에러가 나게 됩니다. 예를들어

```
foo        IN        CNAME   bar
foo        IN        A         10.0.0.1
```

이라고 하면 foo의 주소가 bar의 주소이거나 또는 10.0.0.1 인지 애매한 표현이 되기 때문에
동시에 사용해서는 안됩니다.

7) 로그내용:
couldn't create pid file /chroot/named/var/run/named.pid
조치 =〉 네임데몬 프로세스를 가지고 있는 PID경로가 틀려서 생기는 문제로 named를 재컴파일하도록 권장

8) 로그내용:
db_load could not open: db/db.127.0.0: No such file or directory
조치 =〉 해당 파일이 없어서 나타나는 에러 메세지입니다. /etc/named.conf에 정의된 directory가 /var/named일 경우 실제로 /var/named/db/db.127.0.0 이라는 파일이 없는 경우입니다.
 db.127.0.0 파일의 정확한 경로를 /etc/named.conf에서 해당부분에 변경하시면 됩니다.

9) 로그내용:
Lame server on 'www.candleworks.com' (in 'CANDLEWORKS.com'?): [216.218.131.2].53 'NS2.HE.NET'
조치 =〉 먼저 위의 메세지는 'www.candleworks.com' 을 리졸빙하기 위해서 'NS2.HE.NET'으로 질의를 합니다. 여기서 'NS2.HE.NET'은 CANDLEWORKS.com 에 대한 authority를 가져야 하는 데 그렇지 않아서 발생하는 에러입니다. 잘못된 위임을 뜻하는 것입니다. 이 메세지는 질문하신 분의 네임서버가 잘못되었기 때문이 아니라 CANDLEWORKS.com 에 대한 일차네임서버 지정이 잘못되어 나타나는 것이므로 귀사의 네임서버에는 잘못된 것이 없습니다.
 다만 이 메세지가 많이 나와 보기에 안 좋으시다면 /etc/named.conf에 다음과 같이 해 주신후 네임서버에 HUP 시그널을 보내시면 됩니다.

```
# vi /etc/named.conf
logging {
category lame-servers { null; };
}
# ps -ef |grep named
```

```
# kill -9  pid
```

짧은시간에 이해하시려면 교육을 들으시면 됩니다.^^
[DNS교육] DNS 장애처리 및 보안설정 신청 : http://www.bpan.com/edu_new/edu_lec/49

1.1.1 DNS 자료 사이트

2011.04.10 19:12

1.1.1 DNS 자료 사이트

Internet Systems Consortiumhttp://www.isc.org/

The Team Cymru Web Site http://www.cymru.com/

BIND 9 Administrator Reference Manual http://www.bind9.net/Bv9ARM.html

DNS Q&A Corner http://www.menandmice.com/9000/9310_DNS_Corner_Questions.html

djbdns home page http://www.tinydns.org/

ISP-DNS http://isp-lists.isp-planet.com/isp-dns/0207/index.html#00013

로그 http://www.acmebw.com/askmrdns/bind-messages.htm

짧은시간에 이해하시려면 교육을 들으시면 됩니다.^^
[DNS교육] DNS 장애처리 및 보안설정 신청 : http://www.bpan.com/edu_new/edu_lec/49

1. DNS 용어설명 :피싱(Fishing) Vs 파밍(Pharming)

2011.04.10 19:13

DNS 피싱(Fishing) Vs 파밍(Pharming)

1. 피싱이란 ?

유명한 금융기관 또는 공신력 있는 업체의 이름을 사칭한 **메일을 수신자에게 보내 개인 정보 및 금융정보를 요구하고 이를 이용, 범죄 수단으로 사용하는 것을 말한다.**

2. 파밍이란 ?

등록되어 사용되고 있는 도메인 정보를 변경하여 사용자의 정보를 추출하는 방법

1) 도메인 탈취(등록정보)하는것

2) Address spoofing을 이용한 DNS cache 정보 변경하는것

3) 클라이언트 hosts 파일 변경하여 사이트가 변경되는것

3. 피싱과 파밍의 차이점

1) 피싱은 메일을 받은 특정 수신자가 피해자

2) 파밍은 도메인 자체의 정보가 변경되므로 아무 생각 없이 늘 가는 사이트를 방문했던 사용자들을 속일 수 있기 때문에 피싱의 진화적 형태로 보며 보다 큰 피해가 우려됨

짧은시간에 이해하시려면 교육을 들으시면 됩니다.^^

[DNS교육] DNS 장애처리 및 보안설정 신청 : http://www.bpan.com/edu_new/edu_lec/49

1-1 DNS 구조의 이해

2011.04.10 19:14

1-1 DNS 구조의 이해

1. Root DNS
전세계에 13개 Root가 있습니다.

2. TLD종류
1) gTLD: com, net, org, aero, biz, coop, info, museum, name, pro
2) ccTLD : ISO 3166 2자리 국가코드 (IANA, http://www.iana.org/root-whois/index.html)
3) 기타 iTLD, sTLD
RFC 1591 - http://www.rfc-editor.org/rfc/rfc1591.txt

3. Domain 생성

1) Size limits : UDP messages 512 octets or less
2) Character : a-z, A-Z, 0-9, '-', 대소문자 구분 없음 (언더바는 안됨)
RFC1035 http://www.rfc-editor.org/rfc/rfc1035.txt

짧은시간에 이해하시려면 교육을 들으시면 됩니다.^^
[DNS교육] DNS 장애처리 및 보안설정 신청 : http://www.bpan.com/edu_new/edu_lec/49

1-2 Root DNS가 13개인 이유?

2011.04.10 19:15

1. ROOT DNS

DNS 프로토콜의 응답 패킷인 사용자 데이터그램 프로로콜(UDP) 내부에 수용된 서버 수의 최대치가 13이기 때문에 전 세계에서 오직 13대의 대형 컴퓨터에만 루트 DNS가 존재한다.

1997년 8월 WIDE 프로젝트는 아시아 지역 유일의 루트 DNS 운용을 일본에서 담당하도록 하였으며, 10대는 미국, 나머지 2대는 노르웨이와 네덜란드가 각각 운용하고 있다

DNS Root FAQ : http://www.isoc.org/briefings/020/

2. 왜? 최대치가 13대일까요 ?
ROOT 13대가 넘어가면 DNS질의시 사용되는 메시지 사이즈가 512바이트를 넘어가게됩니다.
DNS는 UDP를 사용하나 512바이트를 넘어가면 TCP로 재질의하게 되어 있습니다.
ROOT에서부터 재질의가 많이 일어나면 부하로 서비스가 안되겠지요 ^^

```
localhost ~]$ dig . ns
; <<>> DiG 9.4.1 <<>> . ns
;; global options: printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 42346
;; flags: qr rd ra; QUERY: 1, ANSWER: 13, AUTHORITY: 0, ADDITIONAL: 13
;; QUESTION SECTION:
;.                      IN      NS
;; ANSWER SECTION:
.               392312  IN      NS      M.ROOT-SERVERS.NET.
.               392312  IN      NS      A.ROOT-SERVERS.NET.
.               392312  IN      NS      B.ROOT-SERVERS.NET.
.               392312  IN      NS      C.ROOT-SERVERS.NET.
.               392312  IN      NS      D.ROOT-SERVERS.NET.
.               392312  IN      NS      E.ROOT-SERVERS.NET.
.               392312  IN      NS      F.ROOT-SERVERS.NET.
.               392312  IN      NS      G.ROOT-SERVERS.NET.
.               392312  IN      NS      H.ROOT-SERVERS.NET.
.               392312  IN      NS      I.ROOT-SERVERS.NET.
```

```
.                       392312  IN      NS      J.ROOT-SERVERS.NET.
.                       392312  IN      NS      K.ROOT-SERVERS.NET.
.                       392312  IN      NS      L.ROOT-SERVERS.NET.
;; ADDITIONAL SECTION:
M.ROOT-SERVERS.NET.     478712  IN      A       202.12.27.33
A.ROOT-SERVERS.NET.     478712  IN      A       198.41.0.4
B.ROOT-SERVERS.NET.     478712  IN      A       192.228.79.201
C.ROOT-SERVERS.NET.     478712  IN      A       192.33.4.12
D.ROOT-SERVERS.NET.     478712  IN      A       128.8.10.90
E.ROOT-SERVERS.NET.     478712  IN      A       192.203.230.10
F.ROOT-SERVERS.NET.     478712  IN      A       192.5.5.241
G.ROOT-SERVERS.NET.     478712  IN      A       192.112.36.4
H.ROOT-SERVERS.NET.     478712  IN      A       128.63.2.53
I.ROOT-SERVERS.NET.     478712  IN      A       192.36.148.17
J.ROOT-SERVERS.NET.     478712  IN      A       192.58.128.30
K.ROOT-SERVERS.NET.     478712  IN      A       193.0.14.129
L.ROOT-SERVERS.NET.     478712  IN      A       198.32.64.12
;; Query time: 8 msec
;; SERVER: 210.116.105.184#53(210.116.105.184)
;; WHEN: Wed Oct 17 22:25:16 2007
;; MSG SIZE  rcvd: 436      <-----메시지 사이즈
```

짧은시간에 이해하시려면 교육을 들으시면 됩니다.^^

[DNS교육] DNS 장애처리 및 보안설정 신청 : http://www.bpan.com/edu_new/edu_lec/49

1. 최신 Root DNS 정보 - http://www.root-servers.org/

2011.04.10 19:16

1. 최신 Root DNS정보 - http://www.root-servers.org/

ROOT IP 변경정보
Date Subject
2007-11-01 New IP address for l.root-servers.net. (199.7.83.42)
2004-01-29 New IP address for b.root-servers.net. (192.228.79.201)

2. 최신 Root 정보 다운로드

[root@isp-dns /etc]# ftp ftp.rs.internic.net 또는 ftp ftp.internic.net 로 해보세요.
Name (ftp.rs.internic.net:root): ftp
Password: 〈엔터〉
ftp〉 cd domain
ftp〉 ascii
ftp〉 ha
Hash mark printing on (1024 bytes/hash mark).
ftp〉 get named.root (이름이 hint file이름이 named.ca 또는 root.hint이면 이름변경하시면 됩니다.)

실무에서 낮은 OS에서는 B.ROOT-Servers.net ,L.ROOT-Servers.net 정보가 예전 IP로 되어 있어,
로그에 Root 대한 경고메시지가 나옵니다.
13개의 Root가 있으므로 서비스에 지장이 없으나 root정보 파일을 수정코자할 경우는 위처럼 새 root 정보파일을 받으면 됩니다.

// 예전 Root IP 정보를 가지고 있는 경우 서버의 남게되는 경고로그
13-Nov-2007 12:02:48.133 general: warning: checkhints: view external: l.root-servers.net/A (199.7.83.42) missing from hints
13-Nov-2007 12:02:48.133 general: warning: checkhints: view external: l.root-servers.net/A (198.32.64.12) extra record in hints
09-Nov-2007 02:18:48.376 general: warning: checkhints: view external: l.root-servers.net/A (199.7.83.42) missing from hints

완료후 반드시 해당 서버에서 # dig @127.0.0.1 www.sun.com 등으로 서비스가 잘되는지 확인하세요. ^^

3. 기존 Root DNS 13개 IP Address - 10개 미국, 3개 기타나라

Server Name IP Location City Country
A.ROOT-SERVERS.NET.198.41.0.4(38.9881,-77.4755) SterlingUnited States

B.ROOT-SERVERS.NET.192.228.79.201(33.9777,-118.4351) Marina Del Rey United States
C.ROOT-SERVERS.NET 192.33.4.12(38.9144,-77.0763) Washington United States
D.ROOT-SERVERS.NET.128.8.10.90(38.8336,-76.8777) College Park United States
E.ROOT-SERVERS.NET.192.203.230.10(34.6325,-86.6527) Huntsville United States
F.ROOT-SERVERS.NET.192.5.5.241(37.4914,-122.211) Redwood City United States
G.ROOT-SERVERS.NET.192.112.36.4(38.9036,-77.4512) Chantilly United States
H.ROOT-SERVERS.NET.128.63.2.53(39.0007,-76.973) Hyattsville United States
I.ROOT-SERVERS.NET.192.36.148.17(59.3333,18.05) Stockholm Sweden
J.ROOT-SERVERS.NET.192.58.128.30(38.9881,-77.4755) Sterling United States
K.ROOT-SERVERS.NET.193.0.14.129(51.3667,6.0833) Root Netherlands
L.ROOT-SERVERS.NET.198.32.64.12(33.9777,-118.4351) Marina Del Rey United States
M.ROOT-SERVERS.NET.202.12.27.33(36,138) Japan

ROOT DNS 동작상태 보는 사이트
http://dnsmon.ripe.net/dns-servmon/server/
http://www.cymru.com/monitoring/dnssumm/

짧은시간에 이해하시려면 교육을 들으시면 됩니다.^^
[DNS교육] DNS 장애처리 및 보안설정 신청 : http://www.bpan.com/edu_new/edu_lec/49

1-3. 국내 Root DNS Mirror 정보

2011.04.10 19:18

1-3. 국내 Root DNS Mirror 정보

ROOT 미러사이트는 인터넷 대란이후 국내에 설치되고 있습니다.
국내에서 ROOT DNS를 찾을때 미국등 해외로 질의하지 않고, 국내 미러서버로 질의하게 됩니다.
이런경우 해외라인이 문제가 생겨도 국내 인터넷서비스는 정상적으로 서비스됩니다.

사실 해외라인이 안된다고 해서 국내 인터넷이 안된다는건 문제는 구조였습니다.
원래 미국에서 DNS설계시 DNS처음 패킷은 ROOT-DNS(미국)에 있는 서버로 가게 되어있습니다.

1. F-미러서버 - 한국인터넷진흥원에 설치. .com .net
2003년 8월 미국의 ISC의 F-미러서버가 도입돼 한국인터넷진흥원에 설치

2. J 루트 미러서버 -KT 분당 인터넷데이터센터(IDC)에서 운영 (2004/10/19)

3. M Root 미러 - 도곡동 KINX 에 위치

짧은시간에 이해하시려면 교육을 들으시면 됩니다.^^
[DNS교육] DNS 장애처리 및 보안설정 신청 : http://www.bpan.com/edu_new/edu_lec/49

1-4 Root DNS 모니터링 사이트 및 공격기사

2011.04.10 19:19

1. Root DNS 모니터링 사이트

1-1. root 동작 모니터링 사이트 : http://dnsmon.ripe.net/dns-servmon/server/

1-2. root 동작 모니터링 사이트 2 http://www.cymru.com/monitoring/dnssumm/

2. Root DNS에 대한 공격

루트 DNS서버 공격 : 2007-0206 "루트 DNS서버 공격, 한국 아닌 독일에서 시작됐다"…정통부 2007-02-13 14:21]

http://www.inews24.com/php/news_view.php?g_serial=248363&g_menu=020100

다음페이지 http://cafe.naver.com/dnspro/888

짧은시간에 이해하시려면 교육을 들으시면 됩니다.^^

[DNS교육] DNS 장애처리 및 보안설정 신청 : http://www.bpan.com/edu_new/edu_lec/49

1-5. DNS 네임서버 $TTL시간은 10분정도로 설정 하는것을 권장한다

2011.04.10 19:20

1. DNS 네임서버 $TTL시간은 10분정도로 설정 하는것을 권장한다.
실무에서 가장 큰문제가 생기는 부분은 회사네임서버에서 Cache를 길게 잘못지정한경우
네임서버에서 IP를 잘못 바꾸었을시, ISP Cache에 정보가 업데이트 된경우이다.
ISP Cache DNS는 시간이 다 지날때까지는 IP에 대한 변경정보가 업데이트 되지 않는다는것이다.

2. 국내구성의 이해

국내 특정ISP의 경우는 UDP 53포트만 서비스한다. TCP 53번은 막혀있다.
네임서버 NS레코더가 7개이상이거나, A 레코더가 30개이상되면 dns패킷사이즈가 512바이트를 넘게되어, 특정 ISP에서는 서비스 되지 못한다.

DNS는 기본적으로 UDP 53번을 사용합니다.
하지만, 기본DNS Message사이즈인 512바이트를 넘을시 TCP로 재전송요청을 하는데 TCP가 막혀있으면 서비스가 안됩니다.
이는 보안정책이며, 요즘은 L4사용으로 512를 넘는경우가 없습니다.

참고자료 :
〉 dig test.serverchk.com

;; Truncated, retrying in TCP mode. 〈------ TCP로 재요청이 일어났음을 알수 있습니다.
; 〈〈〉〉 DiG 9.4.0a6 〈〈〉〉 test.serverchk.com
;; global options: printcmd
;; Got answer:
;; -〉〉HEADER〈〈- opcode: QUERY, status: NOERROR, id: 469
;; flags: qr rd ra; QUERY: 1, ANSWER: 28, AUTHORITY: 2, ADDITIONAL: 0
;; QUESTION SECTION:
;test.serverchk.com. IN A
;; ANSWER SECTION:
test.serverchk.com. 10 IN A 100.1.1.9
test.serverchk.com. 10 IN A 100.1.1.10
test.serverchk.com. 10 IN A 100.1.1.11
test.serverchk.com. 10 IN A 100.1.1.12
test.serverchk.com. 10 IN A 100.1.1.13
test.serverchk.com. 10 IN A 100.1.1.14
test.serverchk.com. 10 IN A 100.1.1.15

```
test.serverchk.com.    10    IN    A    100.1.1.16
test.serverchk.com.    10    IN    A    100.1.1.17
test.serverchk.com.    10    IN    A    100.1.1.18
test.serverchk.com.    10    IN    A    100.1.1.19
test.serverchk.com.    10    IN    A    100.1.1.20
test.serverchk.com.    10    IN    A    100.1.1.21
test.serverchk.com.    10    IN    A    100.1.1.22
test.serverchk.com.    10    IN    A    100.1.1.23
test.serverchk.com.    10    IN    A    100.1.1.24
test.serverchk.com.    10    IN    A    100.1.1.25
test.serverchk.com.    10    IN    A    100.1.1.26
test.serverchk.com.    10    IN    A    100.1.1.27
test.serverchk.com.    10    IN    A    100.1.1.28
test.serverchk.com.    10    IN    A    100.1.1.1
test.serverchk.com.    10    IN    A    100.1.1.2
test.serverchk.com.    10    IN    A    100.1.1.3
test.serverchk.com.    10    IN    A    100.1.1.4
test.serverchk.com.    10    IN    A    100.1.1.5
test.serverchk.com.    10    IN    A    100.1.1.6
test.serverchk.com.    10    IN    A    100.1.1.7
test.serverchk.com.    10    IN    A    100.1.1.8
;; AUTHORITY SECTION:
serverchk.com.         10    IN    NS    ns2.serverchk.com.
serverchk.com.         10    IN    NS    ns1.serverchk.com.
;; Query time: 15 msec
;; SERVER: 168.126.63.1#53(168.126.63.1)
;; WHEN: Sun Jun 27 01:15:55 2010
;; MSG SIZE  rcvd: 520        <— 요기 512가 넘죠 ..... 위를 보면 TCP로 재요청이 일어났음을 알수 있습니다.
```

짧은시간에 이해하시려면 교육을 들으시면 됩니다.^^

[DNS교육] DNS 장애처리 및 보안설정 신청 : http://www.bpan.com/edu_new/edu_lec/49

1-6. DNS 기본구조 및 동작이해

2011.04.10 19:21

1-6. DNS 기본구조 및 동작이해

PC가 DNS를 지정하여 www.naver.com 질의한경우

1. 로컬 PC의 DNS 캐싱확인을 통해 1차로 ip에 대한 확인을 한다.

1) PC는 우선 자체 PC의 Cache를 확인
해당도메인에 대한 IP정보 있으면 www.naver.com ip로 접속한다.

2) PC IP에 대한 Cache정보가 없으면, PC에서 지정한 DNS에가서 물어본다.
3) PC가 지정한 Local DNS에게 www.naver.com을 질의한다.

2. 이후는 Local DNS(PC에서 지정한 DNS가 해당 사이트에대한 IP를 확인하는 작업으로 진행된다.

1) Local DNS는 ROOT DNS에게 com에 대한 정보를 가진 네임서버를 질의한다.
(Cacheing 되어 있는경우는 질의하지 않고 바로 Local DNS에서 응답을준다)
2) Local DNS는 Com ROOT에게 naver 네임서버의 정보를 질의한다.
(Cacheing 되어 있는경우는 질의하지 않고 바로 Local DNS에서 응답을준다)
3) Local DNS는 네이버 네임서버에게 www.naver.com IP 정보를 질의한다.
(Cacheing 되어 있는경우는 질의하지 않고 바로 Local DNS에서 응답을준다)
4) 네이버 네임서버가 www.naver.com에 대한 IP를 Local DNS에 준다.

3. 다음은 PC에 지정된 DNS가 질의한 PC에 확인한 IP를 알려준다.
Loca DNS는 해당 www.naver.com ip를 PC에서 전달한다.

이후 PC는 www.naver.com IP로 접속시도한다.

짧은시간에 이해하시려면 교육을 들으시면 됩니다.^^
[DNS교육] DNS 장애처리 및 보안설정 신청 : http://www.bpan.com/edu_new/edu_lec/49

1-7. DNS 정보확인 명령어

2011.04.10 19:21

1. Root DNS 정보확인 명령어

dig . ns

2. TLD 네임서버 정보확인 명령어

dig com ns

dig kr ns

dig cn ns

3. .com 도메인에 대한 NS확인

예제) 도메인이 serverchk.com 인 경우

dig @j.gtld-servers.net. serverchk.com ns

whois serverchk.com

4. 해당 네임서버에 A 레코더(IP) 확인법

dig @ns1.google.com www.google.com a

5. 네임서버 정보변경시 업데이트

1) .KR 업데이트가 실시간으로 변경되었습니다.

2) 2007년 12월 변경됨 kr업데이트가 하루에 3번에서 실시간으로 업데이트로 변경됨
네임서버 추가시 바로 업데이트 됩니다.

3) 기존에 .Com은 실시간 업데이트 되고 있었습니다.

6. 작업시 고려사항

DNS서버에 설정된 디폴트 $TTL 고려 (Cache Time 고려)

충분이 줄여놓도록 한다. 10분정도

짧은시간에 이해하시려면 교육을 들으시면 됩니다.^^

[DNS교육] DNS 장애처리 및 보안설정 신청 : http://www.bpan.com/edu_new/edu_lec/49

1-9. DNS동작 패킷자료 (1/2)

2011.04.10 19:22

1-9. DNS동작 패킷자료 (1/2)

PC가 DNS서버서버에 www.sun.com 질문시 DNS 동작 패킷자료 (1/2)

1. Red Hat Enterprise Linux AS release 3 (Taroon Update 6), www.sun.com 접속 동작순서.
PC IP는 10.0.7.22
로컬 DNS서버 10.0.1.43

1) PC가 DNS서버서버에 www.sun.com 질문함
12:27:07.942708 10.0.7.22.1025 > 10.0.1.43.domain: 50280+ A? www.sun.com. (29)

2) DNS서버는 b gtld에 문의함
12:27:07.946702 10.0.1.43.32769 > b.gtld-servers.net.domain: 53924 A? www.sun.com. (29) (DF)
12:27:07.946907 10.0.1.43.32769 > blackhole-2.iana.org.domain: 62673 [1au] PTR? 22.7.0.10.in-addr.arpa. (51) (DF) □// DNS서버는 ptr도 문의함

3) b-root는 DNS서버에 www.sun.com의 ns에 대해 응답함
12:27:07.950029 b.gtld-servers.net.domain > 10.0.1.43.32769: 53924- 0/4/4 (165) (DF)

4) DNS서버는 sun.com ns에 www.sun.com ip물어봄
12:27:07.951133 10.0.1.43.32769 > cltea-ns-1.sun.com.domain: 4618 [1au] A? www.sun.com. (40) (DF)

짧은시간에 이해하시려면 교육을 들으시면 됩니다.^^
[DNS교육] DNS 장애처리 및 보안설정 신청 : http://www.bpan.com/edu_new/edu_lec/49

1-9. DNS동작 패킷확인(2/2)

2011.04.10 19:23

1-9. DNS동작 패킷확인(2/2)

PC가 DNS서버서버에 www.sun.com 질문시 DNS 동작 패킷자료 (1/2)

12:27:08.150778 cltea-ns-1.sun.com.domain 〉 10.0.1.43.32769: 4618 FormErr% [0q] 0/0/0 (12) (DF)
// sun.com ns는 DNS서버에 FormErr뿌림

12:27:08.151022 10.0.1.43.32769 〉 cltea-ns-1.sun.com.domain: 1197 A? www.sun.com. (29) (DF)
// DNS서버는 바로 sun.com ns에 www.sun.com ip또 물어봄

12:27:08.232383 blackhole-2.iana.org.domain 〉 10.0.1.43.32769: 62673 NXDomain*- 0/1/1 (128) (DF)
// 리벌스에 대해 도메인이 아니라고 응답함

12:27:08.234413 10.0.1.43.32769 〉 f3.NSTLD.COM.domain: 24480 [1au] PTR? 30.14.33.192.in-addr.arpa. (54) (DF) □// DNS서버는 리버스 재질의

5) sun.com 네임서버는 www.sun.com에 대한 IP를 로컬 DNS서버에 응답함
12:27:08.350714 cltea-ns-1.sun.com.domain 〉 10.0.1.43.32769: 1197*- 1/4/4 A 72.5.124.61 (188) (DF)

6) 로컬 DNS서버는 PC에 www.sun.com ip 알려줌.
12:27:08.351611 10.0.1.43.domain 〉 10.0.7.22.1025: 50280 1/4/0 A 72.5.124.61 (117) (DF)

7) PC는 웹브라우져를 이용해 www.sun.com에 ip로 접속함.

짧은시간에 이해하시려면 교육을 들으시면 됩니다.^^
[DNS교육] DNS 장애처리 및 보안설정 신청 : http://www.bpan.com/edu_new/edu_lec/49

1. DNS 3가지 구성요소

2011.04.10 19:24

1. DNS 3가지 구성요소

1) Domain Name Space
2) Name Server
3) Resolver (PC)

2. Layer Architecture

1) UDP / TCP 53포트를 둘다 사용한다. RFC1035: http://www.isi.edu/in-notes/rfc1035.txt

- UDP 53포트 : 일반 DNS질의 응답

- TCP 53포트는
1) Zone Transfer시 사용, 2) Message Size가 512보다 클 경우 사용됨
// Zone Transfer 란, Master DNS서버의 정보를 Slave서버가 도메인에 대한 Zone File(데이터 전송)을 받아 갈때 사용되는것을 말한다.
메시지 사이즈 확인법

>dig www.serverchk.com

; <<>> DiG 9.4.0a6 <<>> www.serverchk.com
;; global options: printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 580
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 2, ADDITIONAL: 0
;; QUESTION SECTION:
;www.serverchk.com. IN A
;; ANSWER SECTION:
www.serverchk.com. 60 IN A 210.116.123.25
www.serverchk.com. 60 IN A 211.35.64.72
;; AUTHORITY SECTION:
serverchk.com. 60 IN NS ns2.serverchk.com.
serverchk.com. 60 IN NS ns1.serverchk.com.
;; Query time: 203 msec
;; SERVER: 168.126.63.1#53(168.126.63.1)

;; WHEN: Sat Jun 14 19:24:43 2008
;; MSG SIZE rcvd: 103 〈- 메시지 사이즈

3. Root DNS의 수는 13개인 이유

UDP message 정보안에 담긴 NS 정보가 512 bytes를 넘어는 것 방지를 위해서이다
512 bytes 를 초과하게 되면 TCP 질의가 되어 네임서버의 로드를 증가시킨다.

일반 네임 서버에서는 최대 7개 이상 NS 레코드를 사용하지 않는 것을 권장한다
(넘으면 TCP로 재질의 하여 네임서버의 부하가 증가한다.)

다음페이지 http://cafe.naver.com/dnspro/895

짧은시간에 이해하시려면 교육을 들으시면 됩니다.^^
[DNS교육] DNS 장애처리 및 보안설정 신청 : http://www.bpan.com/edu_new/edu_lec/49

1-10. DNS Resolver & Resolution 용어정의

2011.04.10 19:25

1-10. DNS Resolver & Resolution 용어정의

1. Resolver

1. Resolve란?
DNS를 이용하는 클라이언트(PC)를 말함

역할
네임서버로 query를 보내고,
네임서버로 받은 응답을 해석하고,
정보를 요구한 클라이언트에 정보를 전달한다.

2. Name Resolution

클라이언트인 Resolver가 호스트정보를 query하게 되면 자신이 가지지 않은 정보에 대해서도 Domain Name Space를 뒤져서 알려주게 된다. **이러한 일련의 과정을 Name Resolution이라고 한다.**

3. Caching

Resolver가 한번 요청한 정보에 대해서는 DNS는 버리지 않고 호스트 정보가 가진 TTL만큼 메모리에 가지고 있게 된다. 이러한 동작을 Caching이라고 한다.
Caching은 DNS의 Resolution 속도를 높여주며, 매번 Root 네임서버로 가지 않아도 됨으로 Root 네임서버의 부담을 줄여주게 된다.

짧은시간에 이해하시려면 교육을 들으시면 됩니다.^^
[DNS교육] DNS 장애처리 및 보안설정 신청 : http://www.bpan.com/edu_new/edu_lec/49

1-10. DNS 용어정의 : DNS의 종류

2011.04.10 19:26

1-10. DNS 용어정의 : DNS의 종류

DNS종류는 도메인을 관리하는 네임서버(Master, Slave)와 Cache DNS가 있다.

1. 네임서버

1.1 Master server

1) Master server (O) 라고 불리우며, Primary Server(X), 1차(X) 라고 하지는 않기로 하자.

2) 도메인에 대한 주된 host파일을 유지, 호스트 정보의 변경 및 추가 가능 ,Master server는 하나를 권장함.

1.2 Slave server

1) Master에 설정된 도메인 정보를 받아옴 (zone transfer)

2) Master Server에 대한 백업은 아니다.

3) 여럿 존재 가능.

4) .kr의 Slave들

b.dns.kr, c.dns.kr, d.dns.kr, e.dns.kr, f.dns.kr, g.dns.kr

2. Cache only Server

도메인에 대한 authority data를 가지지 않고 resolving 처리를 위해서만 사용.

일반적으로 ISP DNS가 cache DNS이다. 예) KT 168.126.63.1 외

다음페이지 http://cafe.naver.com/dnspro/897

짧은시간에 이해하시려면 교육을 들으시면 됩니다.^^

[DNS교육] DNS 장애처리 및 보안설정 신청 : http://www.bpan.com/edu_new/edu_lec/49

1-10. DNS 응답의 종류

2011.04.10 19:26

1-10. DNS 응답의 종류

1. Authoritative Answer

Query된 도메인의 네임서버에서 직접 데이터를 얻어 응답을 해줄 경우

authoritative answer:
Name: www.sun.com
Address: 209.249.116.195

2. Non-authoritative Answer
클라이언트의 resolving 요청에 DNS의 cache나 다른네임서버가 가진 데이터로 응답

> www.sun.com
Server: localhost
Address: 127.0.0.1

Non-authoritative answer:
Name: www.sun.com
Address: 209.249.116.195

※ RTT(RoundTrip Time)

§갔다가 되돌아오는 총시간

§BIND가 내부적으로 타 네임서버에 대한 RTT값을 기록하고 있다가, 요청 도메인에 대해 다수의 ns 중 RTT값이 가장 낮은 네임서버로 query한다.

§RTT가 없을 경우 해당 네임서버 전체로 동시에 query를 보내어 빠른 응답을 얻고 RTT도 측정한다. 측정된 후에는 도메인에 대한 요청은 RTT가 가장 낮은 서버로 보내진다.

§한번 질의후 해당 DNS에 대한 RTT가 증가되어 한서버에 부하가 몰리는것을 방지한다.

짧은시간에 이해하시려면 교육을 들으시면 됩니다.^^

[DNS교육] DNS 장애처리 및 보안설정 신청 : http://www.bpan.com/edu_new/edu_lec/49

□1-10. DNS 질의의 종류(Query Type)

2011.04.10 19:27

1-10. DNS 질의의 종류(Query Type)

1.1.8 Recursive (재귀적) 질의, Iterative(반복적) 질의

네임서버가 Recursive 모드로 동작할 때에는, 클라이언트(이를 Stub Resolver 라 합니다.)의 요청에 대해 Namespace를 검색한후 결과를 전달한다.
하지만 Iterative 모드에서는 알 수 없는 질의(자신이 관리하지 않는 도메인에 대한 요청)에 대해, 응답 가능한 NS의 목록을 전달합니다.

네임서버는 Recursive 모드로 동작하며, Iterative 모드는 루트서버와 같이 네임서버를 위한 네임서버(네임서버간의 통신에는 Iterative 모드가 사용됨)에서 과다한 트래픽을 막기위해 사용한다.
또한, 클라이언트는 Iterative 모드로 설정된 네임서버를 사용할 수 없으므로, 네임서버 목록(예:resolv.conf, 윈도우의 DNS 찾기목록)에 추가하여서는 안됩니다.

BIND-4에서는 부트파일에 'options no-recursion'을 추가함으로써, Iterative 모드로 전환할 수 있고,
BIND-8,9 의 경우엔 options 엔트리에 'recursion no;'를 설정합니다.

짧은시간에 이해하시려면 교육을 들으시면 됩니다.^^
[DNS교육] DNS 장애처리 및 보안설정 신청 : http://www.bpan.com/edu_new/edu_lec/49

1-10. DNS 구성요소 - Caching

2011.04.10 19:28

1-10. DNS 구성요소 - Caching

DNS 로 Query되는 데이터 중 실제로 중복되는 것이 많다.
한번 검색한 도메인을 Cache에 유지하여, 같은 Query가 요청될 때 Cache에서 응답을 할 수 있다면 트래픽과 속도측면에서 효율적일 것이다.

1. Positive Caching

1) 일반적으로 이해하고 있는 캐싱을 말한다.
2) 존재하는 도메인에 대한 캐싱이므로 후에 같은 질의가 들어오면 효과적으로 대응
3) Default TTL , RR (Resource Record: SOA,NS,A등) TTL 이 있다.

2. Negative Caching

1) 잘못된 query에 대한 결과를 캐싱하여 불필요한 트래픽 차단
2) Negative caching (Minimum TTL)
3) BIND 4.9, BIND 8, BIND 9 에서 사용됨

1-10. DNS구성요소- Positive Caching , $TTL

2011.04.10 19:28

1-10. DNS구성요소- Positive Caching , $TTL

1.Positive Caching - $TTL

1) 형식 (zone file의 최 상단에 위치)
2) $86400
3) TTL size: 32 bit, (RFC 1035)

Default TTL, 각 호스트별 TTL(RR내)이 설정되지 아니한 경우 이 $TTL에 설정된 값이 적용이 된다.
호스트 IP주소 전체가 변경이 될 경우, 이 부분을 변경한다.
$TTL을 적게 10분정도로 잡아 운영한다.

다음페이지 http://cafe.naver.com/dnspro/901

짧은시간에 이해하시려면 교육을 들으시면 됩니다.^^
[DNS교육] DNS 장애처리 및 보안설정 신청 : http://www.bpan.com/edu_new/edu_lec/49

1-10. DNS구성요소- Positive Caching , RR내의 TTL

2011.04.10 19:29

1-10. DNS구성요소- Positive Caching , RR내의 TTL

2. Positive Caching - RR내의 TTL

1) 형식 (zone file 내의 RR)
www **100** 0IN A 10.10.10.1

2) TTL size: 32 bit, (RFC 1035), 86400초 = 1일

3) Positive Cache

호스트의 IP변경과 TTL
하나의 호스트 IP가 변경이 될 경우, IP변경에 따른 Delay 시간을 줄이기 위해 TTL 조정한다.

named # more allworm.com.zone

```
$TTL    10M
@       IN      SOA     allworm.com. root.allworm.com.  (
                                2005101204 ; Serial
                                28800      ; Refresh
                                14400      ; Retry
                                3600000    ; Expire
                                86400 )    ; Minimum

www1    20      IN      A       10.246.1.3
www2    20      IN      A       10.246.1.4
www3            IN      A       10.246.1.4
```

; 위와 같은 경우 www1과 www2는 20초가 TTL이고, www3는 디폴트 TTL인 10M (10분을 따르게 된다)

10M = 10분
20 = 20초

짧은시간에 이해하시려면 교육을 들으시면 됩니다.^^

[DNS교육] DNS 장애처리 및 보안설정 신청 : http://www.bpan.com/edu_new/edu_lec/49

1-10. DNS구성요소 - Negative Caching , Minimum TTL

2011.04.10 19:30

1-10. DNS구성요소 - Negative Caching , Minimum TTL

3. Negative Caching = Minimum TTL

1) 존재하지 않는 호스트, 또는 오류가 있는 호스트에 대한 Name Caching

2) 형식 (SOA의 Minimum TTL)
@ IN SOA ns.aaa.com. hostmatster.aaa.com. (
2004092401 ; Serial
7200 ; refresh
3600 ; retry
604800 ; expire
3600 ; minimum)

3) 초기 목적: default TTL

4) 현재 목적: negative caching에 대한 시간 적용, 최대 3시간
The remaining of the current meanings, of being the TTL to be used for negative responses, is the new defined meaning of the SOA minimum field.

5) 캐싱되는경우
NODATA : No Data
NXDOMAIN : Non-existent domain

6) 잘못된 query의 경우, 존재하는 호스트에 대한 query보다 반복적으로 Query되는 수가 많다.
해당 Query가 잘못된 것임을 미리 알고 있으므로, 불필요한 트래픽 발생을 줄일 수 있고, 응답시간 면에서도 효과적이다.

다음페이지 http://cafe.naver.com/dnspro/904

짧은시간에 이해하시려면 교육을 들으시면 됩니다.^^

[DNS교육] DNS 장애처리 및 보안설정 신청 :

http://www.bpan.com/edu_new/edu_lec/49

2-2. DNS named.conf

2011.04.10 19:31

2-2. DNS named.conf

Named.Conf 파일

1) 네임서비스의 기본 설정을 하는 파일이다.
named가 시작될 때 제일 먼저 읽는 환경설정 파일

2) 기본 설정 위치 : /etc/

3) 설치시 위치 변경법
bind8 # src/port의 해당 OS의 OS/makefile.set에서 경로변경
bind9 # ./configure □sysconfdir=/usr/local/etc §

4) 서비스 중인 DNS서버에서 Named.conf 위치 확인법

```
# ps -ef |grep named
       root  1055     1  0 17:17:12 ?       0:00 /usr/sbin/named

ns# strings /usr/sbin/named |grep named.conf
    /etc/named.conf
```

짧은시간에 한번에 이해하시려면 교육을 들으시면 됩니다.^^
[DNS교육] DNS 장애처리 및 보안설정 신청 : http://www.bpan.com/edu_new/edu_lec/49

2-2. DNS named.conf

2011.04.10 19:32

2-2. DNS named.conf

1. Named.Conf 파일 형식

```
options {
   directory "/var/named";
   pid-file "/var/named/named.pid";   // named pid 파일을 남길 위치
   version  “Unknown !!” ;   // 버전 숨기는 보안설정

   check-names master ignore ;  // 권장설정
    바인드의 규칙검사 강화로 Zone File에 언더바(_)사용을 기존에는 경고로 처리했으나 ,
    최근버전은 에러로 처리하여 , 해당 도메인이 동작하지 않으므로(rejected), 기존 Host named중
     언더바를 사용하고  있는 경우는 바인드 업그레이드시  주의하여야 한다.
```

2. Named.conf 문법오류 확인 유틸

```
# named-checkconf  named.conf    〈 Enter〉
```

이상이 없으면, 아무런 반응이 없다. ^^

짧은시간에 한번에 이해하시려면 교육을 들으시면 됩니다.^^

[DNS교육] DNS 장애처리 및 보안설정 신청 : http://www.bpan.com/edu_new/edu_lec/49

2-2. DNS Zone File

2011.04.10 19:33

2-2. DNS Zone File

1. RFC1035 정의: http://www.isi.edu/in-notes/rfc1035.txt ,

2. SOA : The Start of a zone of authority

```
$TTL 10M     ; 10분
@ IN SOA ns1.domain.com. dnsmaster.domain.com. (
2005090901; serial
3h ; refresh
1h ; retry
1w ; expire
1h) ; TTL (negative cache)
```

DATA Format

{name} {ttl} [class] type Rdata

예) go 600 IN A 200.1.1.221

3. TYPE의 종류 -RFC 1035, 1183, 1706 http://www.iana.org/assignments/dns-parameters

4. Zone File 문법오류 확인 유틸

```
# named-checkzone  yejin.pe.kr  yejin.pe.kr.zone
zone yejin.pe.kr/IN: loaded serial 2007022202
OK
```

5. 매달 named.conf와 zone을 별도 시스템에 백업해두자

6. Zone파일 예제

```
[root@localhost named]# vi   serverchk.com.zone

$TTL    10M
@            IN SOA  ns1.serverchk.com. root (
                              2007042002      ; serial (d. adams)
                              3H              ; refresh
                              15M             ; retry
                              1W              ; expiry
                              1D )            ; minimum
             IN NS          ns1.serverchk.com.
             IN NS          ns2.serverchk.com.
             IN MX   10     mail.serverchk.com.

                    IN A          200.1.1.10
                    IN A          200.1.1.11
ns1.serverchk.com.      IN A            200.1.177.1
ns2.serverchk.com.      IN A            200.1.2.2
www                  IN A           200.1.1.10
                     IN A           200.1.1.11
mail                  IN A          200.1.1.122
ftp                   IN A          200.1.1.122
serverchk.com.          IN      TXT     "v=spf1  ip4:200.1.177.122  ip4:200.1.177.0/24 ~all"
```

짧은시간에 한번에 이해하시려면 교육을 들으시면 됩니다.^^
[DNS교육] DNS 장애처리 및 보안설정 신청 : http://www.bpan.com/edu_new/edu_lec/49

2-3. DNS 일반적인 운영오류 - Serial number 증가시키기 누락

2011.04.10 19:33

2-3. DNS 일반적인 운영오류 - Serial number 증가시키기 누락

1. Serial number 증가시키기 누락

Master서버에서 zone 파일 update 시 serial number 꼭 1이상 증가시켜야 한다.
Master서버 IP의 Serial이 Slave보다 반드시 커야한다.

Slave서버는 이 Serial번호를 비교해서, Master서버의 Zone파일을 받아올지, 현재 파일을 유지할지 정한다. 정보변경 후 Serial Number를 변경시키지 않으면, Master/Slave 서버 사이에 동기화 문제 발생 가능

Zone File안에 Serial 번호가 있음.

```
$TTL 10m      ; 10분
@ IN SOA      ns1.domain.com. dnsmaster.domain.com. (
2005090901                ;  serial 번호
3h ; refresh
1h ; retry
1w ; expire
1h) ; TTL (negative cache)
```

다음페이지 http://cafe.naver.com/dnspro/908

짧은시간에 한번에 이해하시려면 교육을 들으시면 됩니다.^^
[DNS교육] DNS 장애처리 및 보안설정 신청 :
http://www.bpan.com/edu_new/edu_lec/49

2-3. DNS 일반적인 운영오류- DNS서버위치

2011.04.10 19:34

2-3. DNS 일반적인 운영오류- DNS서버위치

1. DNS서버 위치

1) Master/Slave의 서로 다른 물리적 위치에 있도록 한다
2) Master/Slave의 서로 다른 네트웍 블럭을 가지도록 한다

안되어 있을경우 장애 : 회외 및 일반기업의 경우 문제가 되어 서비스가 단절되는 경우 발생되는 경우가 있었음.

2. Master / Slave의 동작?

1) 1차네임서버, 2차 네임서버의 의미 ? DNS서버에서의 의미? Client에서의 의미는?
도메인등록시 1차,2차 네임서버 2개등록 할경우 동작은 동등하게 50%씩 질의가 들어온다.
1차가 들어오다 다운되면 2차가 서비스되는것은 아니다.
2) 안되어 있을경우 장애 - 단독 네임서버운영 장애시 웹,메일 서비스등 전체서비스에 영향을 미침

3. DNS서버 용도별 분리 필요

1) 네임서버용
도메인 관리용 = 외부 DNS서버의 질의에 응답하는 서버

2) 사용자 서비스용
캐쉬 전용서버 □ 클라이언트의 질의에 응답하는 서버

짧은시간에 한번에 이해하시려면 교육을 들으시면 됩니다.^^
[DNS교육] DNS 장애처리 및 보안설정 신청 : http://www.bpan.com/edu_new/edu_lec/49

2-3. DNS 일반적인 운영오류 - DNS서버교체시 주의점

2011.04.10 19:35

2-3. DNS 일반적인 운영오류 - DNS서버교체시 주의점

4. 서버교체시 주의점

1) 주의: 동일 서버 교체시 라우터에서 ARP가 갱신되지 않아 바로 서비스가 살지 않는 문제가 발생.
예) Unix, Windows서버등 바로 동작안하는 경우 발생

해결법: 네트웍장비에서 ARP갱신필요
서버교체시는 Cisco Router에서 # Clear arp-cache 명령어 주어 Arp갱신할수 있다. (기본은 자동)
라우터 교체시는 서버에서 # arp □d ip (Linux / Unix 계열서버는 자동갱신이 늦으므로, 명령어필요)

5. L4이중화작업시 주의점

1) 도메인등록시 네임서버 2개등록 할경우 동작은 동등하게 50%씩 질의가 들어온다.
2) 이중화 작업시 DNS서버의 경우 IP변경이외에 거의 DNS에서 변경해줄 내용은 없음.
(Zone transfer IP제한 설정은 수정이 필요함)
3) Master , Slave , Slave, Slave 구성을 권장 한다.

4) Alteon L4 설정법 : TCP Health 체크, UDP Enabled
/c/slb/virt 53/service domain
group 1 udp enabled // UDP를 Enable 시킴

6. PIX Firewall (Module)사용중 네임서버작업시 주의점
Bind업그레이드시후 질의가 안되는 문제 발생
DNS설정 변경 또는 PIX의 UDP 로 해결할수 있다.
최근 RFC규약변경으로 BInd 버전은 512바이트를 넘어갈수 있도록 되어 있다.
하지만 보안장비에서는 기존에 DNS패킷은 512바이트로 제한되도록 설정되어 있다. 원래 RFC는 512를 넘지 못한다고 되어 있다.

짧은시간에 한번에 이해하시려면 교육을 들으시면 됩니다.^^
[DNS교육] DNS 장애처리 및 보안설정 신청 : http://www.bpan.com/edu_new/edu_lec/49

2-3. DNS 일반적인 운영오류- EDNS지원

2011.04.10 19:36

2-3. DNS 일반적인 운영오류- EDNS지원

10. DNS의 EDNS지원으로 인한 보안장비와의 트라블슈팅

1) 증상: 바인드 버전 업그레이드후 사이트 접속불가
2) 원인: Cisco PIX의 설정과 EDNS지원문제

3) 해결법

(1) Cisco PIX Fireall 해결법

The Extended DNS (EDNS0) feature adds support for the DNS fixup and support for a UDP DNS response packet greater than 512 bytes.
Support for greater than 512 bytes is defined in RFC 2671.
Prior to this feature, the firewall simply dropped UDP DNS response packets greater than 512 bytes.
On my PIX we do this :
fixup protocol dns maximum-length 4096 as named advertises a 4k UDP buffer.

(2) Unix / Linux 해결법

named.conf
options { edns-udp-size 512; };
// edns-udp-size is available in 9.3.0 / 8.4.0.

(3) Windows 2003 서버 해결법

http://support.microsoft.com/?id=828731
turn off EDNS0 support in Windows Server 2003.
Start a command prompt - Type dnscmd /Config /EnableEDnsProbes 0,
then press ENTER.

짧은시간에 한번에 이해하시려면 교육을 들으시면 됩니다.^^

[DNS교육] DNS 장애처리 및 보안설정 신청 : http://www.bpan.com/edu_new/edu_lec/49

2-4. DNS이중화

2011.04.10 19:37

2-4. DNS이중화

1. 네임서버 권장사항

1) 네임서버는 서로 물리적으로 다른 위치에 놓이는것을 권장함.

2) 서버가 1대 밖에 없거나 다른 위치가 없다면, ISP에 Slave설정요청하여 서비스필요함- 현재 무료

3) 기본적으로 네임서버를 2개이상사용하면 1개 다운시 나머지로 서비스가 잘됨. (기본 이중화 구조임)

2. 네임서버 이중화 작업절차

1) Slave네임서버를 다른 위치에 구축한다.
주의 - 서버설정시 Zone File안에 NS정보는 변경되는 정보로 수정

2) Master네임서버 $TTL시간을 줄여놓는다. 10m 정도로.

3) 도메인 등록기관을 통해, 정보를 변경해야 한다.
.com은 실시간 적용됨.- NS3를 추가하는것은 바로 적용되므로 추가하는것을 권장한다.
.kr도 실시간 (100초) 적용으로 변경됨.
(2007년까지는 하루에 3번 업데이트하므로 업데이트 1시간전 도메인등록기관에 접속해 NS IP를 수정함.
예전엔 .kr업데이트 : 매일 08:00~09:00, 12:00~13:00, 18:00~19:00 에 수행되엇음)

4) 네임서버는 원래 이중화구성이므로 하나만 동작하고 있으면 서비스 지장은 없다.

3. 캐쉬DNS 이중화는 L4아래 구성하도록 한다.

PC 및 일반서버에서는 DNS를 내부 Cache DNS IP로 1개 지정하고 , 2차는 외부 ISP DNS로 지정하도록 한다.

짧은시간에 한번에 이해하시려면 교육을 들으시면 됩니다.^^

[DNS교육] DNS 장애처리 및 보안설정 신청 : http://www.bpan.com/edu_new/edu_lec/49

3-1. DNS 도메인 보안설정 - 도메인관리

2011.04.10 19:37

1. Domain Registration Attacks (도메인 등록공격)

1.1 Domain Hijacking =도메인 등록만기/변경, 등록기관이전등 복잡한 절차를 악용

1) 실제사례들
- 2005년 1월 17(금) 미국 뉴욕의 ISP인 P사의 도메인 변경이 받아들여져 탈취된 사건 알려지지 않는 사람에 의해 탈취당해 이틀동안 모든 비즈니스 서비스 중단
- 2004년 9월 4일 독일의 eBay사이트의 도메인 변경신청이 받아들여져 처리됨.

2) 대책:
- 도메인 Lock신청 - 도메인 등록기관 사이트에 가면 무료로 도메인에대한 lock설정을 제공한다.
가서 클릭만 하면 lock설정이 된다. 이경우 다른 fax나 전화로 바로 변경하지 않도록 하는것이다.
사이트 들어가서 lock설정 해지후 변경할수 있다. 하나의 이중보완장치인셈이다.
계정을 탈취당하면 할수 없지만..
- 도메인 관리(만기일,등록 메일계정관리) - 등록시 지정한 메일계정을 잘 관리한다. 쉽게 얘기해 도메인 등록한 메일계정으로 메일을 계속 수신할수 있고, 내용을 확인할수 있도록 해야한다.
담당자가 퇴사로 메일계정이 변경된경우 반드시 변경이 필요하다.

1.2 Similar Domain name registrations - 유사도메인 등록

대책: 사이트에 주의공지, 유사도메인 사전 등록.
예제) www.yaho.com
현재는 yaho도 야후가 보유하고 있다.

1.3 Botnet name server registrations - 악성코드로 인한 감염

1) 아직까지 악성코드로 인한 감염이 늘고 있고, 가장 손쉬운 방법입니다.
=〉 host.file 변조 플러그인.

- 2007년 1월: 스웨덴 최대 은행 '노르디아' 의 고객 250명은 거금 800만 크로나(약 10억6600만 원)를 강탈
- 2007년 영국 바클레이스 은행 , 미국 아메리칸익스프레스 카드, 세계 최대의 인터넷 경매업체 이베이 고객PC정보 유출
- 2007년 2월 :국내에서도 xx은행, xx은행과 xx의 인터넷뱅킹 고객 5000명의 공인인증서 해킹

2) 대책

PC에 치료/방지 프로그램설치 - 무료 프로그램인 알약, 네이버 툴바설치시 도 제공.. 동시에 설치하지 않도록은 한다. 실시간 감시기능으로 무척 느려진다.
tcp view나 process explorer로 주기적인 PC모니터링

짧은시간에 한번에 이해하시려면 교육을 들으시면 됩니다.^^
[DNS교육] DNS 장애처리 및 보안설정 신청 : http://www.bpan.com/edu_new/edu_lec/49

3-1. DNS 도메인 관리법

2011.04.10 19:38

3-1. DNS 도메인 관리법

2. Domain configuration Attacks - 불필요한 메일 링크 클릭금지, 관리 강화

2.1 Dns Wildcards =〉 메일이나 사이트에 숨겨진 링크 클릭금지

예) http://www.mybank.com.Login.html.123123123.pharmer.com
해당 사이트는 mybank가 아니라 pharmer.com 에서 지정한 사이트로 가게된다.
대책: 첨부된 메일의 링크 클릭실행금지

2.2 Poorly Managed DNS Servers - 도메인 관리를 제대로 하지 않는경우

□대책:

- 네임서버 NS설정관리
도메인등록기관에 호스트 ns를 지정한 서버에서 제대로 서비스하는지 확인이 필요하다.
등록시 설정한 ns와 실제 서버상의 네임서버설정이 같아야 한다.
www.serverchk.com 에서 무료점검가능하다.

- 만료일 점검 - 실제로 만료일이 지나서 갑자기 서비스 안되는경우가 있다.
도메인등록시 설정한 메일계정으로 메일이 잘 오는지 확인이 필요하다.
대부분 연장신청건이 메일로만 발송되기 때문이다.

짧은시간에 한번에 이해하시려면 교육을 들으시면 됩니다.^^
[DNS교육] DNS 장애처리 및 보안설정 신청 : http://www.bpan.com/edu_new/edu_lec/49

3-2. DNS BIND자체 취약점 1

2011.04.10 19:39

기존 OS에서 제공되는 Bind버전은 모두 취약버전이다.

1) 구버전은 대부분 취약버전이다. (OS 디폴트 제공버전 = 취약버전)

2) 최신버전 : http://www.isc.org/downloads/all

예) Name: "BIND: Multiple DoS vulnerabilities
Added 2006.09.06] CVE: CVE-2006-4095, CVE-2006-4096Versions affected:
All previous releases of BIND 9.3.x and 9.4.x. See note regarding BIND 9.2.x
Severity:HIGH
Exploitable:Remotely
Type:Denial of Service
Description:
SIG Query Processing:
Recursive servers:
Queries for SIG records will trigger a assertion failure if more than one SIG (covered) RRset is returned.
Exposure can be minimized by restricting sources that can ask for recursion.
Fix:
Upgrade to BIND 9.4.0b2, BIND 9.3.3rc2, BIND 9.3.2-P1, BIND 9.2.7rc1 or BIND 9.2.6-P1 (or later).

다음페이지 http://cafe.naver.com/dnspro/916

짧은시간에 한번에 이해하시려면 교육을 들으시면 됩니다.^^
[DNS교육] DNS 장애처리 및 보안설정 신청 : http://www.bpan.com/edu_new/edu_lec/49

3-2. DNS BIND자체 취약점 2

2. Name: "BIND: Negative Cache DOS" A/K/A "negcache" □[Added 2004.02.04]

Versions affected: All BIND 8 versions prior to 8.4.3, 8.3.7.
Except vendor-only releases 8.1.3, 8.2.2-P8, 8.2.4-P1, 8.2.5-P1. Severity: SERIOUS Exploitable: RemotelyType: Denial of Service
Description:
□An attacker must configure a name server to return authoritative negative responses for a given target domain. Then, the attacker must convince a victim user to query the attacker's maliciously configured name server. When the attacker's name server receives the query, it will reply with an authoritative negative response containing a large TTL (time-to-live) value. If the victim's site runs a vulnerable version of BIND 8, it will cache the negative response and render the target domain unreachable until the TTL expires.
□Workarounds:
□대책: Disable recursion if possible, or limit recursion to specific clients.

3. NTX 버그: buffer overflow

1) 취약버전: BIND8.2, 8.2P1, 8.2.1 (BIND8.2 부터 NTX RR 사용)

2) 특징
NTX RR에 대한 적절한 확인을 하지 못하는 버그이며, 이것을 이용하여 외부에서 buffer overflow시켜 임의의 code를 수행하게 해 named 실행하는 권한의 쉘을 획득

3) 예제: ./t666 해킹코드로 네임데몬권환(root) 획득이 가능하다.

4) 대책: 최신버전으로 업그레이드 =〉〈?xml:namespace prefix = p ns = "urn:schemas-microsoft-com:office:powerpoint" />〈?xml:namespace prefix = p />〈?xml:namespace prefix = p />http://www.isc.org/index.pl?/sw/bind/

4. Inverse Query: buffer overflow

1) 취약버전: BIND4.9.7 이전 버전, BIND8.1.2 이전 버전

2) 특징
외부의 Inverse Query 요청에 대한 응답 수행 시 메모리에서 적절한 한계 값 검사를 하지 않으므로 buffer overflow 취약성이 존재. 공격자가 교묘히 조작한 패킷을 전송하여 root권한을 획득할 수 있다.

3) 대책

최신버전으로 업그레이드, fake-iquery no; 옵션을 사용

짧은시간에 한번에 이해하시려면 교육을 들으시면 됩니다.^^

[DNS교육] DNS 장애처리 및 보안설정 신청 : http://www.bpan.com/edu_new/edu_lec/49

3-2. DNS 버전관리- Bind버전 결정

2011.04.10 19:41

3-2. DNS 버전관리- Bind버전 결정

1. 네임서버를 어떤 버전으로 업그레이드 할것인가?

Root서버 Bind버전 (2007.03.04일 현재)
a.root-servers.net198.41.0.4
b.root-servers.net192.228.79.201 BIND: 9.3.2
c.root-servers.net192.33.4.12 BIND: 8.4.6-REL
d.root-servers.net128.8.10.90 BIND: 9.3.2-P1
e.root-servers.net192.203.230.10 BIND: 9.2.3
f.root-servers.net192.5.5.241 BIND: 9.3.2-P1
g.root-servers.net192.112.36.4 BIND:
h.root-servers.net128.63.2.53 BIND: NSD 3.0.4
i.root-servers.net192.36.148.17 BIND: contact infonetnod.se
j.root-servers.net192.58.128.30 BIND: VGRS4
k.root-servers.net193.0.14.129 BIND: NSD 2.2.1
l.root-servers.net198.32.64.12 BIND: NSD 3.0.3
m.root-servers.net202.12.27.33 BIND: 9.3.3

2. 최신 Bind Download
Bind: http://www.isc.org/
ftp ftp.isc.org
cd isc

짧은시간에 한번에 이해하시려면 교육을 들으시면 됩니다.^^
[DNS교육] DNS 장애처리 및 보안설정 신청 : http://www.bpan.com/edu_new/edu_lec/49

1. BIND의 버전정보는 스캔공격으로 해킹의 사전단계이다.

2011.04.10 19:41

1. BIND의 버전정보는 스캔공격으로 해킹의 사전단계이다.

2. BIND버전 원격으로 확인방법

1) # dig @200.1.1.1 txt chaos version.bind
dig @ns.xxx.com. txt chaos version.bind

2) # nslookup □q=txt □class=chaos version.bind ns.xxx.com

3) C:₩〉 nslookup

〉 server ns.xxx.com

〉 set class=chaos

〉 set type=txt

〉 version.bind

Server: ns.xxx.com

Address: x.x.x.x

VERSION.BIND text = "No!!"

3. BIND 버전 정보 수정

1) # vi /etc/named.conf

options { version " No! " ; // 추가 };

또는

2) 소스컴파일전 수정하여 컴파일

vi ./src/Version

No!

짧은시간에 한번에 이해하시려면 교육을 들으시면 됩니다.^^

[DNS교육] DNS 장애처리 및 보안설정 신청 : http://www.bpan.com/edu_new/edu_lec/49

3-3. DNS 질의제한, Zone정보보호

2011.04.10 19:42

3-3. DNS 질의제한, Zone정보보호

1. 질의제한

```
# vi /etc/Named.conf
options {
        allow-query  { 192.168.10.34; 200.1.1.0/24;  };    <- 추가
};
```

또는

```
# vi /etc/Named.conf
acl "trusted" {
   200.1.1.0/24;
  127.0.0.1;
  //any;
 };  일반적으로 any를 사용하여 모두 질의허용, 설정된 IP외에서는 해당서버를 이용해 질의할수 없음.

options {
        allow-query {   trusted;  };
};
```

2. Zone 정보 보안

```
# vi /etc/named.conf
options {
        allow-transfer  { 127.0.0.1;   Slave네임서버ip; Slave네임서버ip;  };
};
```

예제)

```
options {
      allow-transfer  { 127.0.0.1; 210.1.1.2; 210.1.2.2;  };    <- 이부분 추가
};
```

또는

```
# vi /etc/named.conf

acl "xfer" {
        //none;  // Allow no transfers. If we have other  - Slave네임서버의 경우는 none으로.
        200.1.1.2;  // Allow no transfers. If we have other
                    // name servers, place them here.
};
options {
     allow-transfer {  xfer;  };
};
```

짧은시간에 한번에 이해하시려면 교육을 들으시면 됩니다.^^

[DNS교육] DNS 장애처리 및 보안설정 신청 : http://www.bpan.com/edu_new/edu_lec/49

3부. DNS서버의 보안설정- 용도별 분리

2011.04.10 19:43

3부. DNS서버의 보안설정- 용도별 분리

1. DNS서버 용도별분리

DNS서버는 도메인을 관리하는 네임서버용도와 PC의 DNS로 지정해 사용하는 Cache DNS용도로 구분되어 사용하여야 장애가 줄어 들수 있다.

1) 도메인관리용 서버로 설정하기

설정법:

```
# vi  /etc/named.conf
options
{  recursion no;
};
```

2) 자신이 호스팅하고 있는 도메인에 대한 DNS응답만 처리한다.

3) 스푸핑(spoofing)공격을 방지할수 있다.

Address Spoofing

공격자가 공격대상 DNS서버로 하여 미리 잘못 설정된 자신이 DNS서버로 호스트 정보를 검색하도록 하고 거짓된 응답 정보를 제공한다. 타깃 DNS서버는 검색결과를 cache하게 되면, 이후 해당 도메인의 호스트들은 위조된 cache 결과를 사용하여 인터넷으로 사용하게 되는 방법으로 유명 전자상거래 사이트와 똑같은 내용의 사이트를 만들어 놓고, 일반 사용자의 접속을 유도한 뒤 사용자 ID/PASSWD 등의 정보를 유출할 수 있음

대응책:

recursive query를 규제하거나, use-id-pool yes; 옵션으로 어렵게 할 수 있다.

Use-id-pool :안전한 서버운영을 위해 네임서버가 질의와 응답에 붙이는 메시지 id를 랜덤한 순서로 만든다.

2. Dynamic Update 관리

Default로 실행이 되지 않음, 보안상 사용하지 않음을 권장함.

다음페이지 http://cafe.naver.com/dnspro/921

짧은시간에 한번에 이해하시려면 교육을 들으시면 됩니다.^^
[DNS교육] DNS 장애처리 및 보안설정 신청 : http://www.bpan.com/edu_new/edu_lec/49

3-4. DNS 보안관리. View,TSIG

2011.04.10 19:44

3-4. DNS 보안관리. View,TSIG

1. View 이용한 보안강화
BIND 9에선 recursive query 규제 ,
복수개의 DNS를 분리하여 사용하는 것이 효과적이다.
IP주소에 따라 view에서 응답이 틀리게 설정한다.

하나는 recursion yes , 다른 하나는 recursion no;

```
view "internal" {
match-clients { 200.1.1.0/24; };
recursion yes;
zone "domain.com" {
type master;
file "domain.com_secure.zone"
                                };
};

view "external" {
match-clients { any; };
recursion no;        // 외부에서 recursion제한.
zone "domain.com" {
type master;
file "domain.com.zone"
                          };
};
```

짧은시간에 한번에 이해하시려면 교육을 들으시면 됩니다.^^
[DNS교육] DNS 장애처리 및 보안설정 신청 : http://www.bpan.com/edu_new/edu_lec/49

3-4. DNS 보안관리 - TSIG 설정

2011.04.10 19:45

3-4. DNS 보안관리. TSIG

1. TSIG 이용한 보안강화

1) TSIG (Transaction Signature) 인증으로 보안 강화
2) BIND8.2 이후 버전에서 TSIG를 이용하여 zone transfer를 암호화해서 인증가능함.
3) TSIG는 2대의 네임서버간 시간 동기를 요구하며, Key의 네임이 반드시 일치해야 함

4) master/slave 2대 이상 사용시에만 필요
5) 시간동기화: 5분 이상 차이 시 expired
6) dnssec-keygen 를 사용 key 생성

dnssec-keygen □a HMAC-MD5 □b 128 □n HOST key_name

Master 서버의 named.conf

```
key xxx-seoul. {
algorithm hmac-md5;
secret "mZiMNOUY== ";
};

zone "domain.com" {
type master;
file "domain.com.zone" ;
allow-transfer { key xxx-seoul; };
};
```

Slave 서버의 named.conf

```
key xxx-seoul. {
algorithm hmac-md5;
secret "mZiMNOUY== ";
};
```

```
server 111.111.111 {
transfer-format many-answers;
keys { xxx-seoul.; };
};

Zone “domain.com” {
type slave;
file “domain.com.bak” ;
allow-transfer { none; };
};
```

짧은시간에 한번에 이해하시려면 교육을 들으시면 됩니다.^^

[DNS교육] DNS 장애처리 및 보안설정 신청 :

http://www.bpan.com/edu_new/edu_lec/49

5부. DNS 필수점검 항목

2011.04.10 19:45

1. 네임서버 버전 노출점검

원격에서 네임서버 버전을 확인 가능하도록 설정되어 있는지 점검

=> 버전이 낮은경우 취약점이 노출되어 있어 해당취약점으로 문제가 됨.

```
# dig @ns1.serverchk.com txt chaos version.bind +short
"9.3.6-P1-RedHat-9.3.6-4.P1.el5_5.3"
```

2. Open DNS 점검

외부에서 아무나 DNS사용을 할수 있으면 점검

=> 원격에서 DNS를 다운시키거나 취약점을 이용해 파밍을 시킬수 있음,

```
# dig @ns1.serverchk.com www.nate.com +short
211.234.241.212
```

3. NS정상 여부점검

=> 잘못설정 되어 있으면 서비스가 안되거나, 질의가 늦거나, 외부에서 사이트나 메일수신 잘 안됨.

```
# dig @e.gtld-servers.net serverchk.com
; <<>> DiG 9.3.2 <<>> @e.gtld-servers.net serverchk.com
; (1 server found)
;; global options:  printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 4211
;; flags: qr rd; QUERY: 1, ANSWER: 0, AUTHORITY: 2, ADDITIONAL: 2
;; QUESTION SECTION:
;serverchk.com.                 IN      A
;; AUTHORITY SECTION:
serverchk.com.          172800  IN      NS      ns1.serverchk.com.
serverchk.com.          172800  IN      NS      ns2.serverchk.com.
;; ADDITIONAL SECTION:
ns1.serverchk.com.      172800  IN      A       210.116.123.25
ns2.serverchk.com.      172800  IN      A       211.35.65.68
```

4. NS서버가 동일 네트웍(스위치)으로 구성되어 있는지 점검

=> 스위치하나가 죽으면, 전체서비스가 안됨

```
 # dig @e.gtld-servers.net serverchk.com
; <<>> DiG 9.3.2 <<>> @e.gtld-servers.net serverchk.com
; (1 server found)
;; global options:  printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 4211
;; flags: qr rd; QUERY: 1, ANSWER: 0, AUTHORITY: 2, ADDITIONAL: 2
;; QUESTION SECTION:
;serverchk.com.              IN      A
;; AUTHORITY SECTION:
serverchk.com.         172800  IN      NS      ns1.serverchk.com.
serverchk.com.         172800  IN      NS      ns2.serverchk.com.
;; ADDITIONAL SECTION:
ns1.serverchk.com.     172800  IN      A       210.116.123.25
ns2.serverchk.com.     172800  IN      A       211.35.65.68
```

5. $TTK 값의 적절여부 점검

=> 특히 $TTL 시간을 10분정도로 줄여놓도록 한다.

```
 # dig @ns1.serverchk.com www.serverchk.com
; <<>> DiG 9.3.2 <<>> @ns1.serverchk.com www.serverchk.com
; (1 server found)
;; global options:  printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 35695
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL: 1
;; QUESTION SECTION:
;www.serverchk.com.             IN      A
;; ANSWER SECTION:
www.serverchk.com.      10      IN      A       211.35.65.68
```

6. 서버간의 동기화 여부 점검

시리얼번호의 동일한지 확인필요 => Master-Slave가 제대로 동기화되는지 점검될수 있다.

```
[root@mail /]# dig @ns1.serverchk.com www.serverchk.com soa
; <<>> DiG 9.3.2 <<>> @ns1.serverchk.com www.serverchk.com soa
; (1 server found)
;; global options:  printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 23226
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 0
```

```
;; QUESTION SECTION:
;www.serverchk.com.          IN      SOA
;; AUTHORITY SECTION:
serverchk.com.       10     IN      SOA     ns1.serverchk.com. root.serverchk.com. 2010061007 10800 900 604800 180
;; Query time: 3 msec
;; SERVER: 210.116.123.25#53(210.116.123.25)
;; WHEN: Sat Jan  8 21:08:40 2011
;; MSG SIZE  rcvd: 80

[root@mail /]# dig @ns2.serverchk.com www.serverchk.com soa
; <<>> DiG 9.3.2 <<>> @ns2.serverchk.com www.serverchk.com soa
; (1 server found)
;; global options:  printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 11096
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 0
;; QUESTION SECTION:
;www.serverchk.com.          IN      SOA
;; AUTHORITY SECTION:
serverchk.com.       10     IN      SOA     ns1.serverchk.com. root.serverchk.com. 2010061007 10800 900 604800 180
;; Query time: 2 msec
;; SERVER: 211.35.65.68#53(211.35.65.68)
;; WHEN: Sat Jan  8 21:08:51 2011
;; MSG SIZE  rcvd: 80
```

7. TCP OPEN 점검

=> 막힌경우 512바이트가 넘는건 질의를 못하죠 . 특정 ISP의 경우 보안상 막혀있음.

```
 # dig test.serverchk.com
;; Truncated, retrying in TCP mode.
; <<>> DiG 9.3.2 <<>> test.serverchk.com
;; global options:  printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 47071
;; flags: qr rd ra; QUERY: 1, ANSWER: 33, AUTHORITY: 0, ADDITIONAL: 0
;; QUESTION SECTION:
;test.serverchk.com.          IN      A
;; ANSWER SECTION:
test.serverchk.com.     10      IN      A       100.1.1.7
```

```
test.serverchk.com.    10    IN    A    100.1.1.8
test.serverchk.com.    10    IN    A    100.1.1.9
test.serverchk.com.    10    IN    A    100.1.1.10
test.serverchk.com.    10    IN    A    100.1.1.11
test.serverchk.com.    10    IN    A    100.1.1.12
test.serverchk.com.    10    IN    A    100.1.1.13
test.serverchk.com.    10    IN    A    100.1.1.14
test.serverchk.com.    10    IN    A    100.1.1.15
test.serverchk.com.    10    IN    A    100.1.1.16
test.serverchk.com.    10    IN    A    100.1.1.17
test.serverchk.com.    10    IN    A    100.1.1.18
test.serverchk.com.    10    IN    A    100.1.1.19
test.serverchk.com.    10    IN    A    100.1.1.20
test.serverchk.com.    10    IN    A    100.1.1.21
test.serverchk.com.    10    IN    A    100.1.1.22
test.serverchk.com.    10    IN    A    100.1.1.23
test.serverchk.com.    10    IN    A    100.1.1.24
test.serverchk.com.    10    IN    A    100.1.1.25
test.serverchk.com.    10    IN    A    100.1.1.26
test.serverchk.com.    10    IN    A    100.1.1.27
test.serverchk.com.    10    IN    A    100.1.1.28
test.serverchk.com.    10    IN    A    100.1.1.29
test.serverchk.com.    10    IN    A    100.1.1.30
test.serverchk.com.    10    IN    A    100.1.1.31
test.serverchk.com.    10    IN    A    100.1.1.32
test.serverchk.com.    10    IN    A    100.1.1.33
test.serverchk.com.    10    IN    A    100.1.1.1
test.serverchk.com.    10    IN    A    100.1.1.2
test.serverchk.com.    10    IN    A    100.1.1.3
test.serverchk.com.    10    IN    A    100.1.1.4
test.serverchk.com.    10    IN    A    100.1.1.5
test.serverchk.com.    10    IN    A    100.1.1.6
;; Query time: 133 msec
;; SERVER: 8.8.8.8#53(8.8.8.8)
;; WHEN: Sat Jan  8 21:10:40 2011
;; MSG SIZE  rcvd: 564
```

8. MX 리버스 등록여부점검

=〉 리버스 안되어 있으면 메일 송신 문제발생, 상대가 수신거부할수 있음.

```
# dig -x 203.255.112.34 +short
ns.higlobe.net.
```

```
[root@mail named]# dig -x 203.255.112.35 +trace
; <<>> DiG 9.3.2 <<>> -x 203.255.112.35 +trace
;; global options:  printcmd
.                       8373    IN      NS      a.root-servers.net.
.                       8373    IN      NS      b.root-servers.net.
.                       8373    IN      NS      c.root-servers.net.
.                       8373    IN      NS      d.root-servers.net.
.                       8373    IN      NS      e.root-servers.net.
.                       8373    IN      NS      f.root-servers.net.
.                       8373    IN      NS      g.root-servers.net.
.                       8373    IN      NS      h.root-servers.net.
.                       8373    IN      NS      i.root-servers.net.
.                       8373    IN      NS      j.root-servers.net.
.                       8373    IN      NS      k.root-servers.net.
.                       8373    IN      NS      l.root-servers.net.
.                       8373    IN      NS      m.root-servers.net.
;; Received 228 bytes from 8.8.8.8#53(8.8.8.8) in 125 ms
203.in-addr.arpa.       86400   IN      NS      SEC1.AUTHDNS.RIPE.NET.
203.in-addr.arpa.       86400   IN      NS      TINNIE.ARIN.NET.
203.in-addr.arpa.       86400   IN      NS      NS3.APNIC.NET.
203.in-addr.arpa.       86400   IN      NS      NS4.APNIC.NET.
203.in-addr.arpa.       86400   IN      NS      DNS1.TELSTRA.NET.
203.in-addr.arpa.       86400   IN      NS      NS1.APNIC.NET.
;; Received 193 bytes from 198.41.0.4#53(a.root-servers.net) in 203 ms
255.203.in-addr.arpa.   86400   IN      NS      b.dns.kr.
255.203.in-addr.arpa.   86400   IN      NS      f.dns.kr.
255.203.in-addr.arpa.   86400   IN      NS      g.dns.kr.
255.203.in-addr.arpa.   86400   IN      NS      c.dns.kr.
255.203.in-addr.arpa.   86400   IN      NS      d.dns.kr.
255.203.in-addr.arpa.   86400   IN      NS      e.dns.kr.
;; Received 147 bytes from 193.0.9.3#53(SEC1.AUTHDNS.RIPE.NET) in 320 ms
112.255.203.in-addr.arpa. 43200 IN      NS      ns3.epidc.co.kr.
112.255.203.in-addr.arpa. 43200 IN      NS      ns2.epidc.co.kr.
;; Received 92 bytes from 61.74.75.1#53(b.dns.kr) in 3 ms
112.255.203.in-addr.arpa. 86400 IN      SOA     ns2.epidc.co.kr. domain.epnetworks.co.kr. 2005062801 21600 1800 1209600 86400
;; Received 114 bytes from 211.115.194.3#53(ns3.epidc.co.kr) in 3 ms
```

9. Spf 설정여부 점검

=〉 메일문제발생, 설정이 안되어 있으면, 메일송신시 상대가 수신 거부

```
# dig txt serverchk.com +short
"v=spf1 ip4:211.35.65.68 ip4:210.116.123.25 ~all"
```

10. 네임서버의 숫자의 적절성 점검

=〉 일반적으로 2개이상 운영하여야 한다.

```
 # dig @e.gtld-servers.net serverchk.com
; <<>> DiG 9.3.2 <<>> @e.gtld-servers.net serverchk.com
; (1 server found)
;; global options:  printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 4211
;; flags: qr rd; QUERY: 1, ANSWER: 0, AUTHORITY: 2, ADDITIONAL: 2
;; QUESTION SECTION:
;serverchk.com.              IN      A
;; AUTHORITY SECTION:
serverchk.com.        172800  IN      NS      ns1.serverchk.com.
serverchk.com.        172800  IN      NS      ns2.serverchk.com.
;; ADDITIONAL SECTION:
ns1.serverchk.com.    172800  IN      A       210.116.123.25
ns2.serverchk.com.    172800  IN      A       211.35.65.68
```

다음페이지 http://cafe.naver.com/dnspro/11270

짧은시간에 한번에 이해하시려면 교육을 들으시면 됩니다.^^

[DNS교육] DNS 장애처리 및 보안설정 신청 : http://www.bpan.com/edu_new/edu_lec/49

DNS 소프트웨어 사용률

2011.04.10 19:47

http://dns.measurement-factory.com/surveys/sum1.html

57% run the most recent, secure versions of BIND (9.x):

BIND 9.3, 9.2, 9.1	57%
BIND 8.3, 8.2, 8.1	20%
Windows 2000	6.5%
Windows 2003	3.5%
Other	13%

http://mydns.bboy.net/survey/

70.105%	24,335,752	BIND
15.571%	5,405,266	TinyDNS
6.237%	2,165,143	Microsoft DNS Server
2.792%	969,097	MyDNS
1.964%	681,614	PowerDNS
1.250%	433,905	Simple DNS Plus
1.138%	395,206	Unknown
0.277%	96,232	Pliant DNS Server
0.203%	70,455	NSD
0.144%	49,921	UltraDNS
0.104%	36,195	Net::DNS::Nameserver
0.083%	28,656	QuickDNS
0.064%	22,087	Incognito DNS Commander
0.025%	8,508	MaraDNS
0.024%	8,174	rbldnsd
0.018%	6,135	Totd
0.001%	386	ATLAS
0.001%	371	Posadis
0.001%	312	NonSequitur DNS
0.000%	12	Nominum ANS/CNS

짧은시간에 한번에 이해하시려면 교육을 들으시면 됩니다.^^

[DNS교육] DNS 장애처리 및 보안설정 신청 : http://www.bpan.com/edu_new/edu_lec/49

DNS기초에서 보안까지 !!!

블로그 여행을 떠나다 !!! http://blog.daum.net/topasvga

저자 여행을떠나다

발행일 2011.09.23 01:01:10

Daum 블로그