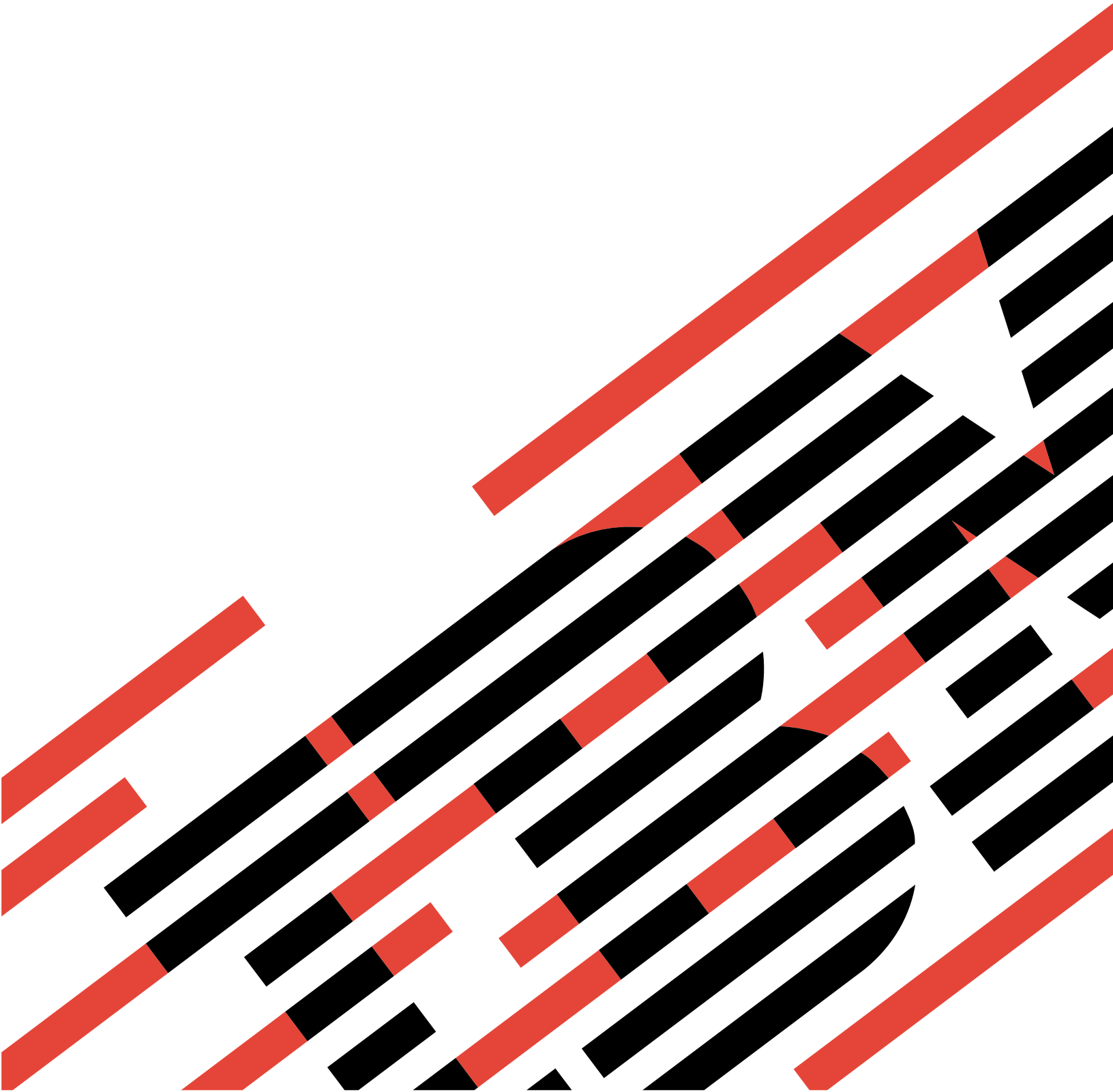
IBM

eserver

iSeries

DNS



IBM

@server

iSeries

DNS

목차

DNS

정의역명 시스템(DNS)은 호스트명과 관련 인터넷 프로토콜(IP) 주소를 관리하기 위한 분산 데이터베이스 시스템입니다. DNS를 사용하면 IP 주소(xxx.xxx.xxx.xxx)를 사용하지 않고 ″www.jkltoys.com″과 같은 간단한 이름을 사용하여 호스트를 찾을 수 있습니다. 단일 서버는 존 서브세트의 IP 주소와 호스트명만 알면 되지만, DNS 서버는 모든 정의역명을 IP 주소에 맵핑하기 위해 함께 작업할 수 있습니다. DNS 서버가 함께 작업하는 것은 컴퓨터가 인터넷을 통해 통신할 수 있도록 하는 것입니다.

버전 5 릴리스 1(V5R1)의 경우 DNS 서비스는 BIND(Berkeley Internet Name Domain) 버전 8이라는 업계 표준 DNS 구현을 기반으로 한 것입니다. 이전 OS/400(R) DNS 서비스는 BIND 4.9.3을 기반으로 하고 있습니다. 신규 BIND 8 기반의 DNS 서버를 사용하려면 iSeries(TM) 서버에 OS/400 옵션 33, PASE(Portable Application Solutions Environment)를 설치하십시오. PASE를 사용하지 않더라도 이전 릴리스에서 사용할 수 있었던 BIND 4.9.3 기반의 동일한 DNS 서버를 실행할 수 있습니다.

주: 이 주제에서는 BIND 8을 기반으로 한 신규 피처를 설명합니다. BIND 8을 기반으로 한 DNS를 실행하기 위해 PASE를 사용하지 않을 경우 BIND 4.9.3을 기반으로 한 DNS에 관해 V4R5 Information Center에서 DNS

를 참조하십시오.

- V5R1의 새로운 사항은 OS/400 DNS에 관한 갱신 정보를 설명합니다.
- 이 주제 인쇄를 통해 DNS 주제를 다운로드하거나 인쇄할 수 있습니다.

DNS 이해
이 주제는 iSeries의 DNS 기본사항에 대한 이해를 돕기 위한 것입니다.

DNS 예에서는 다이어그램과 DNS 작동 방식에 대한 설명을 제공합니다.

DNS 개념은 DNS가 올바로 기능하기 위해 사용하는 오브젝트와 프로세스에 관해 설명합니다.

DNS 계획은 DNS 구성 계획을 작성할 때 도움이 됩니다.

DNS 사용
이 주제는 iSeries에서 DNS를 구성하고 관리하는 데 도움을 주기 위한 것입니다. 새로 나온 신규 피처의 이점에 관해서도 설명합니다.

DNS 시스템 요구사항
이 주제에서는 iSeries 서버에서 DNS를 실행하기 위한 소프트웨어 요구사항을 설명합니다.

DNS 구성
이 주제에서는 이름 서버를 구성하고 정의역을 벗어난 조회를 분석하기 위해 iSeries Navigator를 사용하는 방법을 설명합니다.

DNS 관리
이 주제에서는 DNS 기능 확인, 성능 모니터, DNS 자료와 파일의 유지보수 방법에 대해 논의합니다.

DNS 문제 해결
이 주제에서는 DNS 서버를 사용하여 문제점을 해결하는 데 도움을 주는 DNS 기록 및 디버깅 설정 값에 관해 설명합니다.

Information Center에서 답을 찾을 수 없는 의문사항은 기타 DNS 정보에서 제공하는 기타 자원 리스트 및 참조서를 보십시오.

V5R1의 새로운 사항

신규 소프트웨어 피처

버전 5 릴리스 1(V5R1)에서 DNS 인터페이스가 다시 설계되었습니다. V5R1 DNS 서비스는 BIND(Berkeley Internet Name Domain) 버전 8이라는 업계 표준 DNS 구현을 기반으로 한 것입니다. 이전 OS/400 DNS 서비스는 BIND 4.9.3을 기반으로 하고 있습니다.

신규 BIND 8 기반의 DNS 서버를 사용하려면 iSeries 서버에 OS/400 옵션 33, PASE(Portable Application Solutions Environment)를 설치하십시오. 자세한 정보는 DNS 시스템 요구사항을 참조하십시오.

PASE가 없으면, 신규 BIND 8 피처를 이용할 수 없습니다. 그러나 이전 릴리스에서 사용할 수 있었던 BIND 4.9.3을 기반으로 한 동일한 DNS 서버를 실행할 수 있습니다. V4R5 Information Center에서 BIND 4.9.3을 기반으로 한 DNS 관련 정보 DNS

를 참조하십시오.

BIND 8이 지원하는 신규 피처는 동적 갱신입니다. DHCP과 기타 권한이 있는 소스로부터 보안 동적 자원 레코드 갱신을 허용하도록 DNS 서버를 설정할 수 있습니다. BIND 8 피처 주제에서 BIND 8이 지원하는 기타 신규 피처에 관해 설명합니다.

- 단일 시스템의 복수 DNS 서버
- 조건부 이송
- 보안 동적 갱신
- 통지
- 존 증분 전송(IXFR)

신규 정보

V5R1 Information Center DNS 주제가 BIND 8 기반의 신규 DNS 기능을 지원하도록 갱신되었습니다. PASE가 없는 경우 이전 릴리스에서 사용하던 BIND 4.9.3을 기반으로 한 동일한 DNS 서버를 실행할 수 있습니

다. V4R5 Information Center에서 BIND 4.9.3을 기반으로 한 DNS 관련 정보 DNS

를 참조하십시오.

DNS 시나리오는 기본 DNS 개념을 소개하는 예를 제공합니다. iSeries에 DNS를 계획 및 구성할 때 이 시나리오를 참조하십시오. 문제 해결 정보를 사용하여 서버 구성을 디버그할 때 도움을 받을 수 있습니다.

이 주제 인쇄

PDF 버전을 보거나 다운로드하려면 DNS(약 243KB 또는 40 페이지)를 선택하십시오.

PDF를 워크스테이션에 저장하여 보거나 인쇄하려면 다음과 같이 하십시오.

1. 브라우저에서 PDF를 여십시오(위의 링크 클릭).
2. 브라우저 메뉴에서 **파일**을 클릭하십시오.
3. **다른 이름으로 저장...**을 클릭하십시오.
4. PDF를 저장할 디렉토리를 찾으십시오.
5. **저장**을 클릭하십시오.

PDF를 보거나 인쇄하기 위해 Adobe Acrobat Reader가 필요하면 Adobe 웹 사이트 (www.adobe.com/products/acrobat/readstep.html)

에서 사본을 다운로드할 수 있습니다.

DNS 예

DNS는 호스트명과 관련 IP 주소를 관리하기 위한 분산 데이터베이스 시스템입니다. 다음 예는 DNS의 작동 방식과 네트워크에서의 DNS 사용 방법을 설명합니다. 그리고 DNS를 설정하여 사용하는 이유에 관해 설명합니다. 또한 관련이 있는 개념들과의 링크를 통해 사용자의 이해를 돕습니다.

예: 인트라넷용 단일 DNS 서버
내부 사용 목적의 DNS 서버가 있는 간단한 서브네트를 설명합니다.

예: 인터넷 액세스를 가진 단일 DNS 서버
인터넷에 직접 연결된 DNS 서버가 있는 간단한 서브네트를 설명합니다.

예: 동일한 iSeries 서버의 DNS와 DHCP
동일한 서버의 DNS와 DHCP를 설명합니다. 구성을 사용하여 DHCP가 호스트에 IP 주소를 할당할 때 동적으로 DNS 존이 갱신되도록 할 수 있습니다. DHCP 서버가 서로 다른 iSeries에 상주할 때의 추가 DHCP 구성 요구사항은 예: 서로 다른 iSeries 서버의 DNS와 DHCP를 참조하십시오.

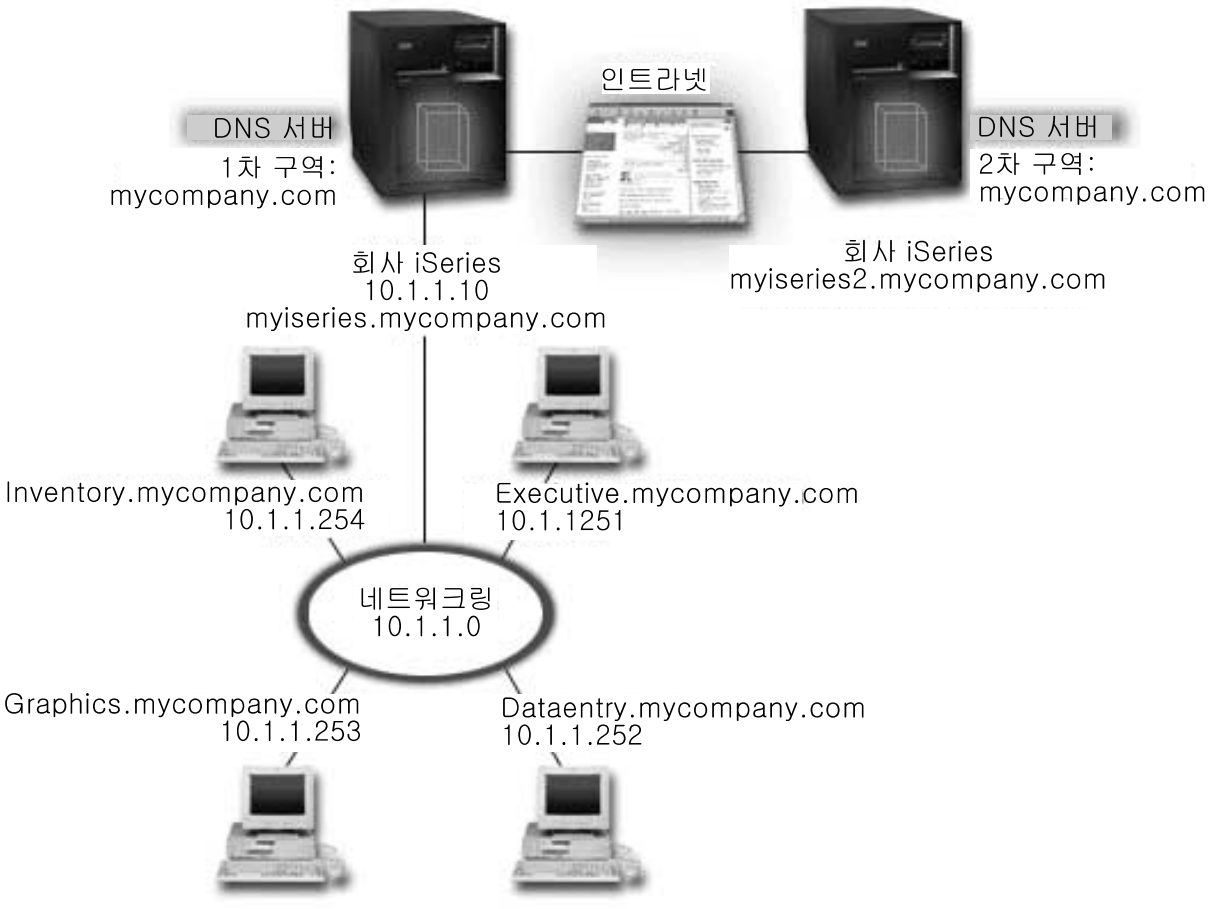
예: 방화벽에서의 분할 DNS

내부 사용자가 인터넷 자료에 액세스할 수 있도록 하는 동시에 인터넷으로부터 내부 자료를 보호하기 위해 방화벽을 통해 작동하는 DNS를 설명합니다.

예: 인트라넷용 단일 DNS 서버

다음 일러스트레이션은 내부 네트워크용으로 iSeries에서 실행되는 DNS를 설명합니다. 단일 DNS 서버 인스턴스는 모든 인터페이스 IP 주소에서 조회를 청취하도록 설정되어 있습니다. 서버는 ″mycompany.com″ 존의 1차 이름 서버입니다.

그림 1. 인트라넷용 단일 DNS 서버.



존의 각 호스트에는 IP 주소와 정의역명이 있습니다. 관리자가 자원 레코드를 작성하여 DNS 존 자료에 호스트를 수동으로 정의해야 합니다. 주소 맵핑(A) 레코드는 기계명을 연관된 IP 주소에 맵핑합니다. 이렇게 하면 네트워크의 기타 호스트가 DNS 서버를 조회하여 특정 호스트명에 할당된 IP 주소를 찾을 수 있습니다. 역방향 검색 포인터(PTR) 레코드는 기계의 IP 주소를 연관된 이름에 맵핑합니다. 이렇게 하면 네트워크의 다른 호스트가 DNS 서버를 조회하여 IP 주소에 대응하는 호스트명을 찾을 수 있습니다.

A 레코드와 PTR 레코드 외에도 DNS는 필요한 여러 가지의 다른 자원 레코드를 지원하는데, 이것은 인트라넷에서 실행 중인 다른 TCP/IP 기반의 어플리케이션에 의해 결정됩니다. 예를 들어, 내부 전자 우편 시스템을 실행 중인 경우에는 SMTP가 DNS를 조회하여 메일 서버를 실행 중인 시스템을 찾을 수 있도록 메일 교환(MX) 레코드를 추가해야 합니다.

이러한 소형 네트워크가 대형 인트라넷의 일부인 경우에는 내부 루트 서버를 정의해야 합니다.

2차 서버

2차 서버는 인증된 서버로부터 존 자료를 로드합니다. 2차 서버는 인증된 서버로부터 존을 전송함으로써 존 자료를 확보합니다. 2차 이름 서버가 시작할 때, 1차 이름 서버로부터 지정된 정의역에 대한 모든 자료가 요구됩니다. 2차 이름 서버는 1차 이름 서버로부터 통지를 수신(NOTIFY (17See) 기능이 사용되고 있는 경우)하거나 1차 이름 서버를 조회하고 자료가 변경되었는지 판별하기 때문에 1차 이름 서버로부터 갱신된 자료를 요구합니다.

위의 그림에서 myiseries 서버는 인트라넷의 일부입니다. 다른 iSeries 서버, myiseries2가 mycompany.com zone에 대한 2차 DNS 서버의 역할을 하도록 구성되었습니다. 2차 서버를 사용하여 서버에 대한 요구에서 균형을 조절할 수 있으며, 1차 서버가 다운될 경우 백업을 제공할 수도 있습니다. 모든 존에는 최소한 하나의 2차 서버를 두는 것이 좋습니다.

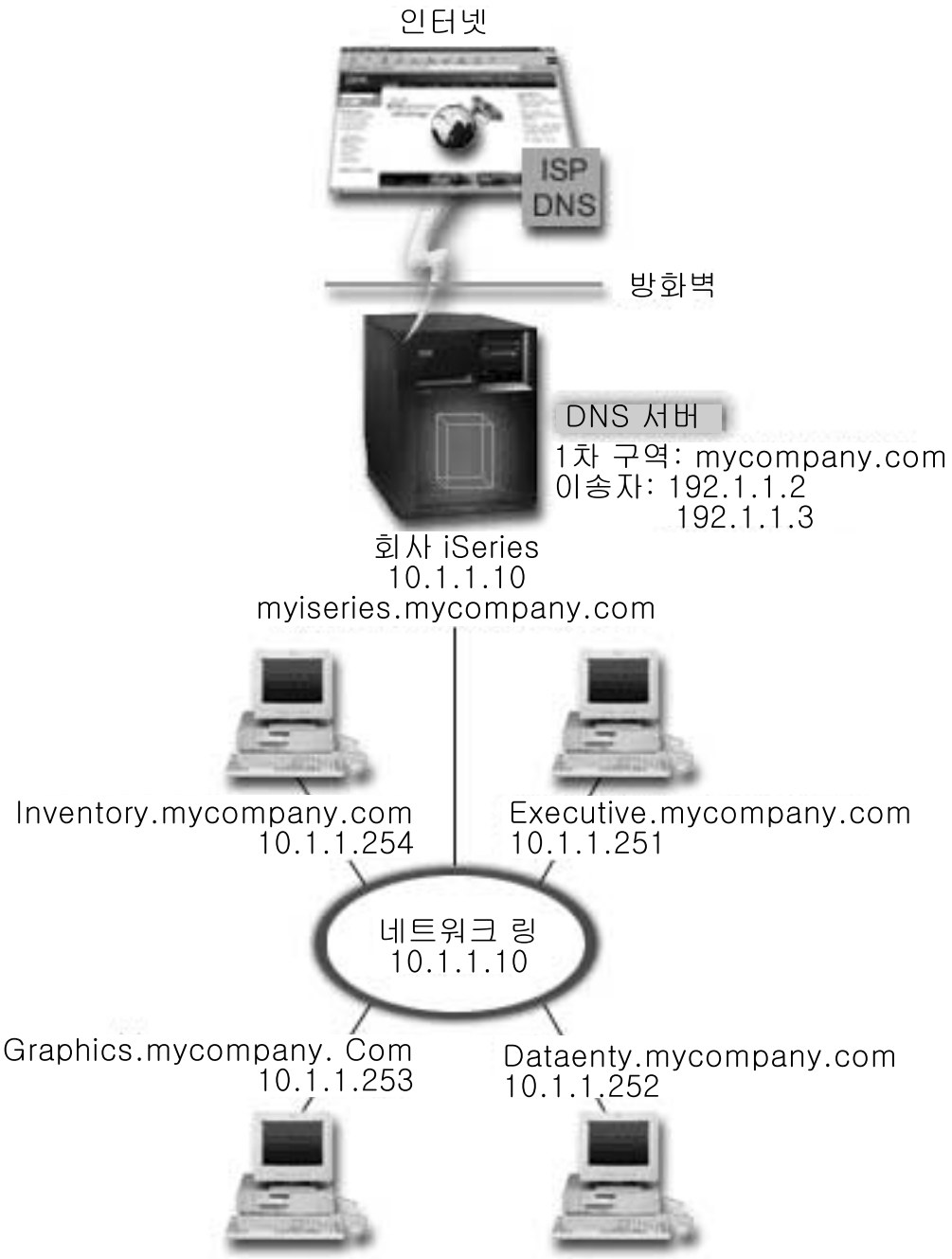
이 예에서 논의된 오브젝트에 대한 자세한 정보는 다음 주제를 참조하십시오.

- DNS 이해는 DNS 정의와 작동 방법을 설명합니다. DNS 서버에 정의할 수 있는 서로 다른 존 유형들도 정의합니다.
- DNS 자원 레코드는 DNS에서 자원 레코드를 사용하는 방법을 설명합니다.

예: 인터넷 액세스를 가진 단일 DNS 서버

다음 일러스트레이션은 인트라넷용 단일 DNS 서버 예와 같은 네트워크의 예를 설명하되 회사에 인터넷 연결이 추가되어 있습니다. 이 예에서, 회사는 인터넷에 액세스할 수 있지만 네트워크로의 인터넷 통신을 차단하기 위해 방화벽이 구성되어 있습니다.

그림 1. 인터넷 액세스를 가진 단일 DNS 서버.



인터넷 주소를 분석하려면 다음 중 최소한 하나를 수행해야 합니다.

인터넷 루트 서버 정의

디폴트 인터넷 루트 서버를 자동으로 로드할 수 있지만 리스트를 갱신해야 합니다. 이 서버는 자신의 존을 벗어난 주소를 분석하는 데 도움이 됩니다. 최신 인터넷 루트 서버를 구하기 위한 지침은 외부 DNS 자료에 액세스를 참조하십시오.

이송 작동 가능

이송을 설정하여 mycompany.com 외부의 존에 대한 조회를 인터넷 서비스 제공자(ISP)가 실행하는 DNS 서버와 같은 외부 DNS 서버로 전달할 수 있습니다. 이송 및 루트 서버 모두로 탐색하기를 원하면 **이송** 옵션을 **first**로 설정해야 합니다. 서버가 먼저 이송을 시도한 다음에 이송이 조회 분석에 실패하면 루트 서버를 조회합니다.

다음과 같은 구성 변경도 필요합니다.

제한되지 않은 IP 주소 지정

위 예에서는 10.x.x.x 주소가 표시됩니다. 그러나 이 주소는 제한된 주소이므로 인트라넷을 벗어나 사용할 수 없습니다. 예를 목적으로 아래 주소를 표시하기는 했으나 ISP 및 기타 네트워킹 요소가 사용자 소유의 IP 주소를 판별할 것입니다.

정의역명 등록

인터넷을 사용할 수 있으나 아직 등록하지 않은 경우에는 정의역명 등록을 해야 합니다.

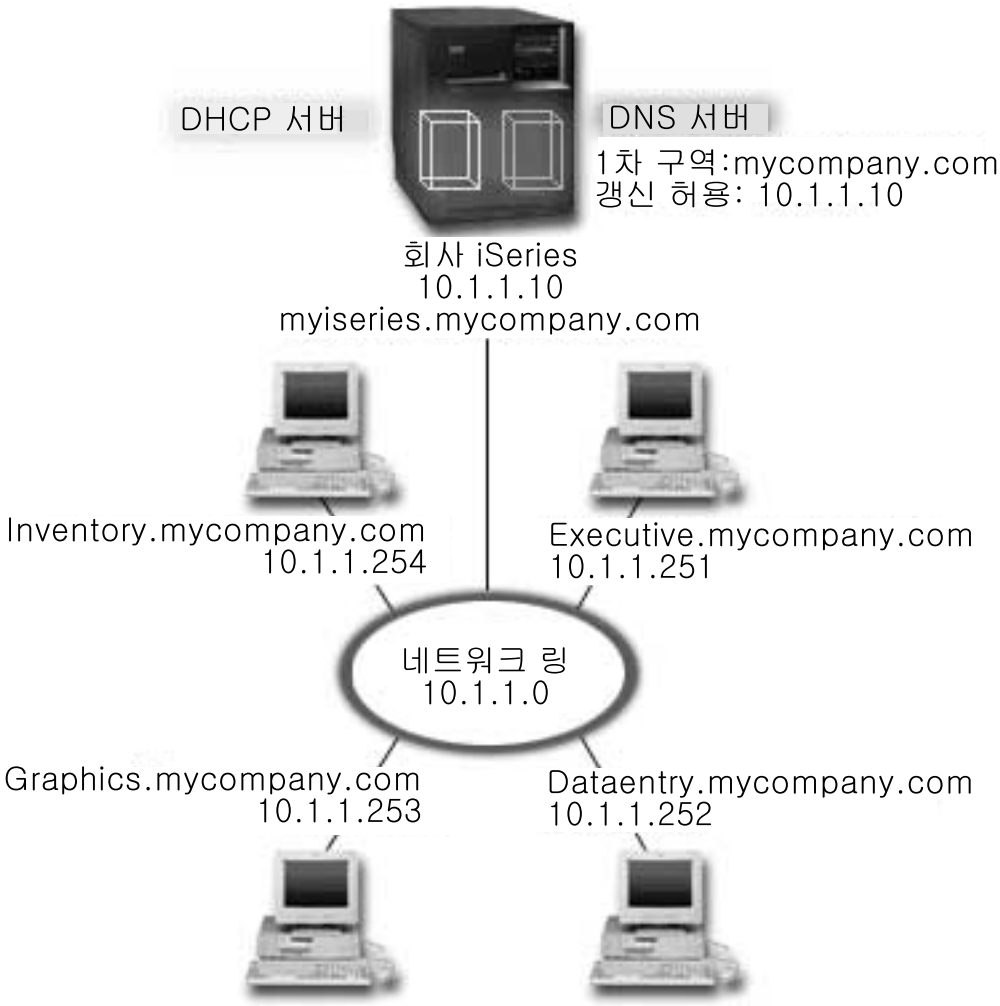
방화벽 설정

DNS를 인터넷에 직접 연결하는 것은 권장되지 않습니다. 방화벽을 구성하거나 다른 예방책을 강구하여 iSeries를 보안해야 합니다. 자세한 정보는 Information Center에서 IBM Secureway: iSeries 및 인터넷을 참조하십시오.

예: 동일한 iSeries 서버의 DNS와 DHCP

다음 그림은 네 개의 클라이언트에 대해 DHCP와 DNS 서버 역할을 하는 iSeries 한 대가 있는 소형 서브네트 네트워크를 설명합니다. 이 작업 환경에서는 명세, 자료 항목, 실행 클라이언트가 그래픽 파일 서버로부터 그래픽이 있는 문서를 작성하는 것으로 가정하십시오. 각 클라이언트는 그 호스트명에 대한 네트워크 드라이브로 그래픽 파일 서버에 연결됩니다.

그림 1. 동일한 iSeries 서버의 DNS와 DHCP.



DHCP와 DNS 이전 버전은 서로 독립적입니다. DHCP가 클라이언트에 신규 IP 주소를 할당한 경우 관리자가 수동으로 DNS 레코드를 갱신해야 했습니다. 이 예의 경우 DHCP가 주소를 지정함으로 인해 그래픽 파일 서버의 IP 주소가 변경되더라도 DNS 레코드에는 파일 서버의 이전 IP 주소가 있기 때문에 종속 클라이언트가 네트워크 드라이브를 호스트명에 맵핑할 수 없습니다.

BIND 8을 기반으로 한 V5R1 DNS 서버를 사용하면 DHCP를 통해 중간 주소와 결합함으로써 DNS 레코드에 동적 갱신을 허용하도록 DNS 존을 구성할 수 있습니다. 예를 들어, 그래픽 파일 서버가 전용 상태를 갱신하고 DHCP 서버가 10.1.1.250이라는 IP 주소를 할당하면 연관 DNS 레코드가 동적으로 갱신됩니다. 이와 같이 할 경우에는 중단시키지 않고 다른 클라이언트가 호스트명별로 그래픽 파일 서버의 DNS 서버를 조회할 수 있습니다.

동적 갱신을 허용하도록 DNS 존을 구성하려면 다음 타스크를 완료하십시오.

동적 존 식별
서버가 실행되는 중에는 수동으로 동적 존을 갱신할 수 없습니다. 수동으로 변경하면 들어오는 동적 갱신을 방해할 수 있습니다. 서버가 중단된 경우에는 수동 갱신을 할 수 있으나 서버가 중단된 상태에서 송

신된 동적 갱신이 유실될 수 있습니다. 이와 같은 이유로 동적 존을 별도로 구성하여 수동 갱신의 필요성을 최소화할 수 있습니다. 동적 갱신 기능을 사용하도록 존을 구성하는 것에 대한 자세한 정보는 정의역 구조 판별을 참조하십시오.

갱신 허용 옵션 구성
갱신 허용 옵션이 구성된 존은 동적 존으로 간주됩니다. 갱신 허용 옵션은 존마다 설정됩니다. 동적 갱신을 허용하려면 이 존에 대해 갱신 허용 옵션을 작동시켜야 합니다. 이 예의 경우 mycompany.com 존에 갱신 허용 자료가 있으나 서버에 정의된 기타 존을 정적 또는 동적으로 구성할 수 있습니다.

동적 갱신을 송신하도록 DHCP 구성
분배된 IP 주소의 경우 DNS 레코드를 갱신할 수 있도록 DHCP 서버에 반드시 권한을 부여해야 합니다. 동적 갱신을 송신하도록 DHCP 서버를 구성하는 것에 대한 자세한 정보는 동적 갱신을 송신하도록 DHCP 구성을 참조하십시오.

2차 서버 갱신 기본설정 구성
2차 서버를 최신 상태로 유지하기 위해서 존 자료가 변경될 때 NOTIFY (17See)를 사용하여 mycompany.com 존의 2차 서버로 메세지를 송신하도록 DNS를 구성할 수 있습니다. 또한 존 증분 전송(IXFR)(17See)을 구성해야 하는데, 존 증분 전송은 IXFR이 가능한 2차 서버를 사용하여 전체 존을 로드하지 않고 갱신된 존 자료만 추적하여 로드합니다.

서로 다른 서버에서 DNS와 DHCP를 실행할 경우 DHCP 서버에 대한 몇 가지의 추가 구성 요구사항이 있습니다. 자세한 정보는 예: 서로 다른 iSeries 서버의 DNS와 DHCP를 참조하십시오.

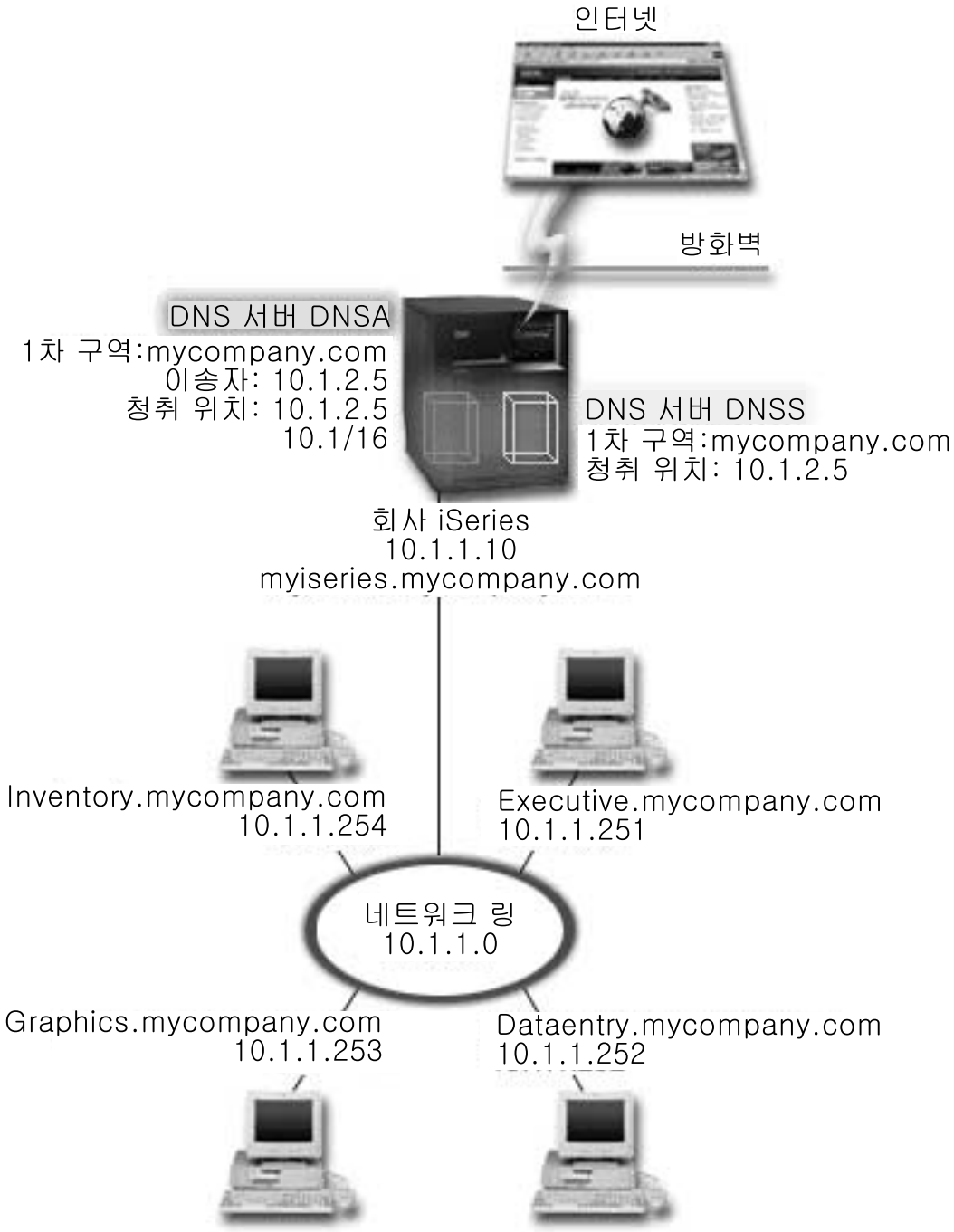
예: 방화벽에서의 분할 DNS

다음 일러스트레이션은 보안을 위해 방화벽을 사용하는 간단한 서브네트 네트워크를 설명합니다. BIND 기반의 V5R1 DNS를 사용하여 단일 iSeries에서 복수 DNS 서버를 설정할 수 있습니다. 회사에 예약된 IP 공간을 가진 내부 네트워크가 있으며, 공용으로 사용할 수 있는 외부 네트워크 섹션이 있는 것으로 가정하십시오.

회사에서는 내부 클라이언트가 외부 호스트명을 분석하고 외부인들과 메일을 교환할 수 있기를 원합니다. 또한 모든 내부 네트워크의 외부에서는 전혀 사용할 수 없는 특정한 내부 전용 존에 내부 분석자들이 액세스할 수 있게 하려고 합니다. 그러나 어떤 외부 분석자들도 내부 네트워크에 액세스하는 것은 원하지 않습니다.

이를 위해 회사에서는 동일한 iSeries에 두 개의 DNS 서버 인스턴스를 설정하되, 하나는 인트라넷용으로 그리고 다른 하나는 공용 정의역의 모든 것을 위해 사용하려고 합니다. 이와 같은 처리를 분할 DNS이라고 합니다.

그림 1. 방화벽에서의 분할 DNS.



외부 서버, DNSB가 1차 존 mycompany.com으로 구성됩니다. 이러한 존 자료에는 공용 정의역의 일부인 자원 레코드만 있습니다. 내부 서버, DNSA는 1차 존 mycompany.com으로 구성되지만, DNSA에 정의된 존 자료에는 인트라넷 자원 레코드가 있습니다. 이송자 옵션은 10.1.2.5로 정의됩니다. 이렇게 하면 DNSA가 분석할 수 없는 조회를 강제로 DNSB 서버로 이송하게 됩니다.

방화벽이나 다른 보안 침입에 대한 무결성을 고려해야 할 경우 내부 자료를 보호하기 위해 청취 옵션을 사용할 수 있는 옵션이 있습니다. 이 옵션을 사용하면 내부 호스트로부터 내부 mycompany.com 존에 대해 조회

만 허용하도록 내부 서버를 구성할 수 있습니다. 이 모든 것이 올바로 작동하기 위해서는 DNSA 서버만 조회하도록 내부 클라이언트를 구성해야 합니다. 분할 DNS를 설정하려면 다음 구성 설정도 고려해야 합니다.

청취
앞에 나오는 예에는 iSeries에 하나의 DNS 서버만 있었습니다. 이 서버는 모든 인터페이스 IP 주소를 청취하도록 설정된 것입니다. iSeries에 복수 DNS 서버를 사용할 때마다 각 서버가 청취하는 인터페이스 IP 주소를 정의해야 합니다. 두 개의 DNS 서버가 동일한 주소를 청취할 수는 없습니다. 이 경우 방화벽으로부터 들어오는 모든 조회가 10.1.2.5로 송신되는 것으로 가정하십시오. 이 조회는 외부 서버로 송신되어야 합니다. 따라서, DNSB는 10.1.2.5를 청취하도록 구성됩니다. 내부 서버, DNSA는 10.1.2.5를 *제외*한 모든 10.1.x.x 인터페이스 IP 주소로부터 조회를 허용하도록 구성됩니다. 이 주소를 효과적으로 제외시키려면 포함된 주소 접두부 앞에 나오는 제외된 주소가 주소 일치 리스트(AML)에 있어야 합니다.

주소 일치 리스트(AML) 순서
주소가 일치하는 AML의 첫 번째 요소가 사용됩니다. 예를 들어, 10.1.2.5를 제외한 10.1.1.x 네트워크의 모든 주소를 허용하려면 ACL 요소 순서가 !10.1.2.5; 10.1/16이어야 합니다. 이 경우 주소 10.1.2.5가 첫 번째 요소와 비교되어 즉시 거부됩니다.

요소가 반전된 경우(10.1/16; !10.1.2.5)에는 서버가 일치하는 첫 번째 요소와 비교한 후 나머지 규칙을 검사하지 않고 허용하기 때문에 IP 주소 10.1.2.5에 액세스가 허용됩니다.

DNS 개념

V5R1 DNS는 BIND 8을 기반으로 한 신규 피처를 제공합니다. 다음의 링크는 DNS 작동 방법 및 사용할 수 있는 신규 피처의 개요를 제공합니다.

기본 DNS 기능:

DNS 이해
사용자가 정의할 수 있는 존 유형에 대한 설명 뿐만 아니라 DNS의 개념과 작동 방법의 개요를 제공합니다.

DNS 조회 이해
DNS가 클라이언트를 대신하여 조회를 분석하는 방법을 설명합니다.

DNS 정의역 설정
사용자 고유 정의역 공간을 설정하기 위한 다른 참조 사이트의 링크와 함께 정의역 등록 개요를 제공합니다.

신규 DNS 피처:

동적 갱신
BIND 8 기반의 V5R1 DNS는 동적 갱신을 지원합니다. 동적 갱신을 사용하여 외부 자원(예: DHCP)이 DNS 서버로 갱신을 송신할 수 있습니다.

BIND 8 피처
동적 갱신 외에도 BIND 8은 DNS 서버 성능을 향상시키기 위한 여러 가지 신규 피처를 제공합니다.

자원 레코드 참조:

DNS 자원 레코드
자원 레코드는 정의역명과 IP 주소 자료를 저장하는 데 사용됩니다. 이 주제에는 V5R1에 지원되는 탐색 가능한 자원 레코드 리스트가 들어 있습니다.

메일 및 MX 자원 레코드
DNS는 이 레코드들을 사용하여 확장 메일 라우팅을 지원합니다.

DNS를 자세히 설명하는 외부 소스가 많이 있습니다. 다른 참조 소스에 대해서는 기타 DNS 정보를 참조하십시오.

DNS 이해

정의역명 시스템(DNS)은 호스트명과 관련 인터넷 프로토콜(IP) 주소를 관리하기 위한 분산 데이터베이스 시스템입니다. DNS를 사용하면 IP 주소(xxx.xxx.xxx.xxx)를 사용하지 않고 ″www.jkltoys.com″과 같은 간단한 이름을 사용하여 호스트를 찾을 수 있습니다. 단일 서버는 존 서브세트의 IP 주소와 호스트명만 알면 되지만, DNS 서버는 모든 정의역명을 IP 주소에 맵핑하기 위해 함께 작업할 수 있습니다. DNS 서버가 함께 작업하는 것은 컴퓨터가 인터넷을 통해 통신할 수 있도록 하는 것입니다.

DNS 자료는 정의역의 계층으로 구분됩니다. 서버들은 하나의 부속 정의역과 같이 자료의 일부분만 알면 됩니다. 서버가 직접 처리하는 정의역 부분을 존이라고 합니다. 전체 호스트 정보와 존에 대한 자료를 가지고 있는 DNS 서버의 경우 그 존에 대해 인증된 것으로 간주됩니다. 인증된 서버는 자신의 자원 레코드를 사용하여 그 존의 호스트에 관한 조회에 응답할 수 있습니다. 조회 처리는 여러 가지 요소에 의해 결정됩니다. DNS 조회 이해는 클라이언트가 조회를 처리하기 위해 사용할 수 있는 경로에 관해 설명합니다.

존 이해
DNS 자료는 존이라고 하는 관리 가능한 자료 세트로 나뉩니다. 존에는 하나 이상의 DNS 정의역 부분에 대한 이름 및 IP 주소 정보가 들어 있습니다. 존에 대한 모든 정보를 가진 서버가 그 정의역에 대해 인증된 서버입니다. 경우에 따라서는 특정 부속 정의역에 대한 DNS 조회에 응답할 수 있는 권한을 다른 DNS 서버에 위임하는 것이 필요할 때가 있습니다. 이 경우 적절한 서버에 대한 부속 정의역 조회를 참조하도록 정의역의 DNS 서버를 구성할 수 있습니다.

백업 및 중복을 목적으로 존 자료를 인증된 DNS 서버가 아닌 다른 서버에 저장하는 경우도 있습니다. 이러한 다른 서버를 2차 서버라고 하며, 인증된 서버로부터 존 자료를 로드합니다. 2차 서버를 구성하면 서버에 대한 요구에 있어서 균형을 조절할 수 있으며, 1차 서버가 중단되더라도 백업을 제공할 수 있습니다. 2차 서버는 인증된 서버로부터 존을 전송함으로써 존 자료를 확보합니다. 2차 서버가 초기화될 때, 1차 서버로부터 전체 존 자료의 사본을 로드합니다. 또한 존 자료가 변경되면 2차 서버가 해당 정의역의 1차 서버 또는 다른 2차 서버로부터 존 자료를 다시 로드합니다.

DNS 존 유형
DNS 자료 관리에 도움이 되도록 iSeries DNS를 사용하여 여러 가지 존 유형을 정의할 수 있습니다.

1차 존
호스트에 있는 파일로부터 직접 존 자료를 로드합니다. 1차 존에 서브존이나 하위 존이 포함되기도 합니다. 또한 호스트, 별명(CNAME), 주소(A) 또는 역 맵핑 포인터(PTR) 레코드 등의 자원 레코드가 포함될 수도 있습니다.
주: 다른 BIND 문서에서는 1차 존을 ″마스터 존″이라고도 합니다.

서브존
서브존은 1차 존 안에 있는 존을 말합니다. 서브존을 사용하여 관리가 가능한 단위로 존 자료를 나누어 구성할 수 있습니다.

하위 존
하위 존은 서브존을 말하며, 서브존 자료에 대한 책임을 하나 이상의 이름 서버에 위임합니다.

별명(CNAME)
별명은 1차 정의역명을 위한 대체명을 말합니다.

호스트
호스트 오브젝트는 A 레코드와 PTR 레코드를 호스트에 맵핑합니다. 추가 자원 레코드를 호스트와 연관시킬 수 있습니다.

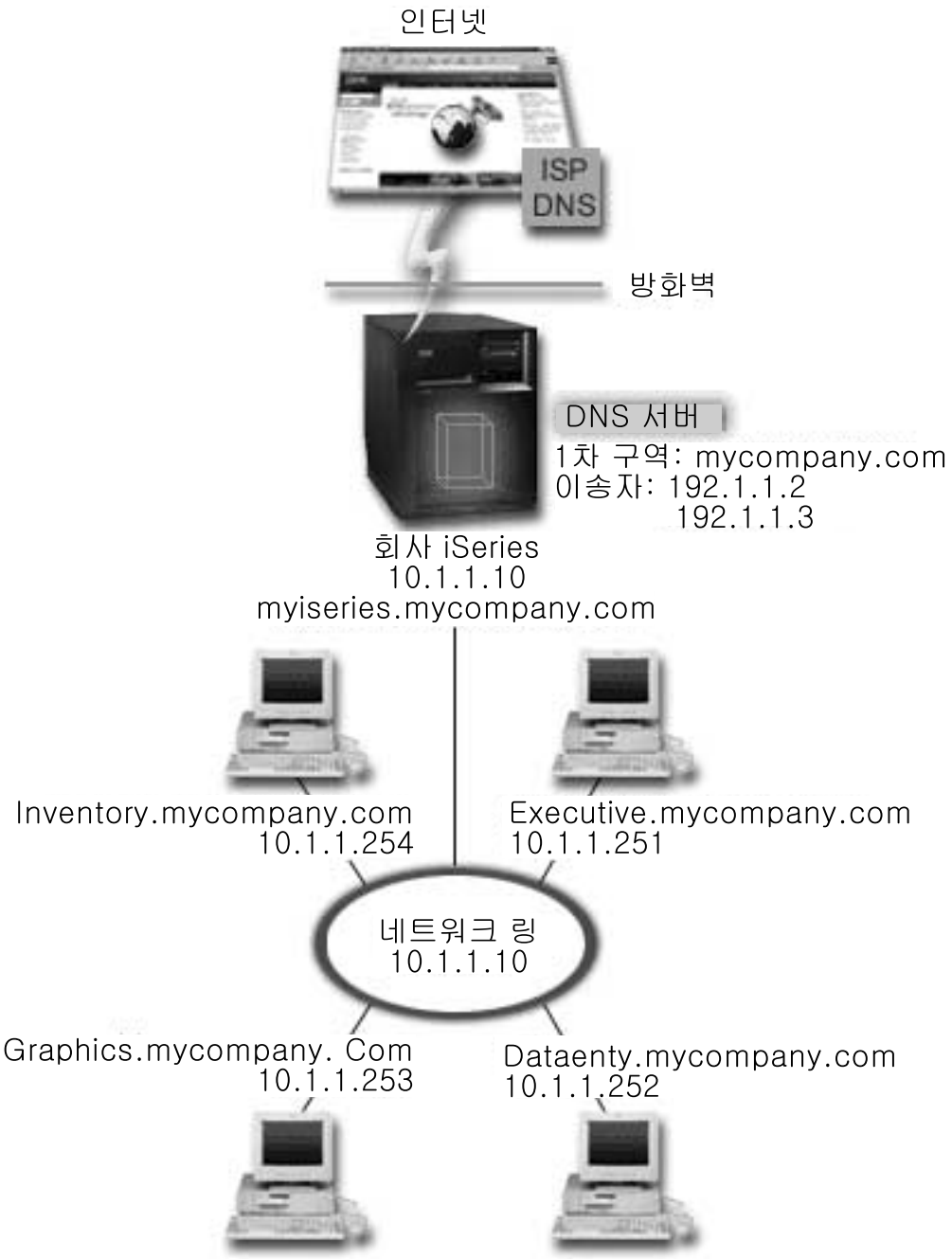
2차 존
존의 1차 서버 또는 다른 2차 서버로부터 존 자료를 로드합니다. 2차 서버는 2차 존을 위한 전체 사본을 유지보수합니다.
주: 다른 BIND 문서에는 2차 존을 ″종속 존″이라고 합니다.

스터브 존
스터브 존은 2차 존과 유사하지만, 그 존에 대한 이름 서버(NS) 레코드를 전송하는 역할만 합니다.

이송 존
이송 존은 특정 존에 대한 모든 조회를 다른 서버로 지시합니다.

DNS 조회 이해
클라이언트는 DNS 서버를 사용하여 서버 정보를 찾습니다. 클라이언트로부터 직접 요구가 나오거나 클라이언트에서 실행 중인 어플리케이션에서 나올 수 있습니다. 클라이언트는 완전 규정 정의역명(FQDN), 클라이언트가 요구한 특정 자원 레코드 등의 조회 유형, 정의역명 클래스(보통, 인터넷(IN) 클래스)가 들어 있는 DNS 서버로 조회 메세지를 송신합니다. 다음 그림은 인터넷 액세스를 가진 단일 DNS 서버의 예를 통해 샘플 네트워크를 설명한 것입니다.

그림 1. 인터넷 액세스를 가진 단일 DNS 서버.



호스트 자료 항목이 "graphics.mycompany.com"의 DNS 서버를 조회하는 것으로 가정하십시오. DNS 서버는 자신의 존 자료를 사용하며, IP 주소 10.1.1.253으로 응답할 것입니다.

이제 자료 항목이 "www.jkl.com."의 IP 주소를 요구하는 것으로 가정하십시오. DNS 서버의 존 자료에는 이 호스트가 없습니다. 이제, 순환 또는 반복의 두 가지 경로를 사용할 수 있습니다. DNS 서버가 순환을 사용하도록 설정된 경우에는 서버가 요구 클라이언트를 대신하여 다른 DNS 서버에 조회하거나 접촉하여 이름을 완전히 분석한 후 다시 클라이언트로 응답을 송신할 수 있습니다. DNS 서버가 다른 DNS 서버를 조회할 경우에는 요구 서버가 응답을 캐싱하여 다음에 그 조회를 수신할 때 사용할 수 있도록 합니다. 또한 클라이언트가

자신을 대신하여 이름을 분석하도록 다른 DNS 서버에 접촉을 시도할 수 있습니다. 반복이라고 부르는 이 프로세스에서는 클라이언트가 서버로부터의 참조 응답을 기반으로 별도의 조회 및 추가 조회를 사용합니다.

DNS 정의역 설정

DNS를 사용하면 인트라넷 또는 내부 네트워크에 이름과 주소를 제공할 수 있습니다. 또한 인터넷을 통해 다른 세계로 이름과 주소를 제공할 수도 있습니다. 인터넷에 정의역을 설정하려면 정의역명을 등록해야 합니다.

인트라넷을 설정할 경우에는 내부 사용을 목적으로 정의역명을 등록하지 않아도 됩니다. 인트라넷명 등록해야 할 것인지는 내부 사용과는별도로 다른 사람이 인터넷에서 그 이름을 사용할 수 있도록 할 것인지에 따라 달라집니다. 사용할 이름을 내부적으로 등록하면 나중에 그 정의역명을 외부적으로 변경하는 경우에 충돌이 전혀 발생하지 않습니다.

권한이 있는 정의역명 등록 기관과 직접 연락하거나 일부 인터넷 서비스 제공자(ISP)를 통해 정의역명을 등록할 수 있습니다. 일부 ISP는 사용자 대신에 정의역명 등록 요구를 제출하는 서비스를 제공합니다. InterNIC(net Network Information Center)

는 ICANN(Internet Corporation for Assigned Names and Numbers)이 공인한 모든 정의역명 등록 기관 목록을 관리합니다.

DNS 정의역을 제공(hosting)하기 위해 등록 및 준비 정보를 제공하는 다른 기관들이 많이 있습니다. 추가 지원 자료는 기타 DNS 정보를 참조하십시오.

동적 갱신

동적 호스트 구성 프로토콜(DHCP)은 중앙 서버를 사용하여 네트워크 전체의 IP 주소와 기타 구성 세부사항을 관리하는 TCP/IP 표준입니다. DHCP 서버는 클라이언트로부터의 요구에 응답하여 클라이언트에 동적으로 등록 정보를 할당합니다. DHCP를 사용하여 중앙 위치에서 네트워크 호스트 구성 매개변수를 정의하고 자동으로 호스트 구성을 수행할 수 있습니다. DHCP는 네트워크에 사용할 수 있는 IP 주소 수보다 클라이언트 수가 더 많은 경우 클라이언트에 임시로 IP 주소를 할당하는 데 자주 이용됩니다.

이전에는 모든 DNS 자료가 정적 데이터베이스에 저장되었습니다. 따라서 관리자가 모든 DNS 자원 레코드를 작성하여 유지보수해야 했습니다. 이제는 존 자료를 동적으로 갱신하기 위해 BIND 8을 실행하는 DNS 서버가 다른 소스로부터의 요구를 허용하도록 구성할 수 있습니다.

호스트에 신규 주소가 할당될 때마다 DNS 서버로 갱신 요구를 송신하도록 DHCP 서버를 구성할 수 있습니다. 이와 같은 자동화된 프로세스는 TCP/IP 네트워크가 급속히 확장되거나 변경될 때 호스트가 자주 위치를 변경하는 네트워크에서의 DNS 서버 관리 작업을 줄여줍니다. DHCP를 사용하는 클라이언트가 IP 주소를 수신하면, 그 자료가 DNS 서버로 즉시 송신됩니다. 이 방법을 사용하면 IP 주소가 변경되더라도 DNS가 호스트에 대한 조회를 계속해서 처리할 수 있습니다.

클라이언트를 대신하여 주소 맵핑(A) 레코드, 역방향 검색 포인터(PTR) 레코드 또는 둘 다 갱신하도록 DHCP를 구성할 수 있습니다. A 레코드는 기계의 호스트명을 그 IP 주소에 맵핑합니다. PTR 레코드는 기계의 IP

주소를 그 호스트명에 맵핑합니다. 클라이언트의 주소가 변경되면, DHCP가 자동으로 DNS 서버로 갱신을 송신하여 네트워크의 기타 호스트가 신규 IP 주소에서 DNS 조회를 통해 클라이언트를 찾을 수 있도록 합니다. 동적으로 갱신된 각 레코드의 경우 DHCP가 레코드를 작성했는지 식별하기 위해 연관된 텍스트(TXT) 레코드가 작성됩니다.
주: PTR 레코드만 갱신하기 위해 DHCP를 설정할 경우에는 클라이언트로부터의 갱신을 허용하도록 DNS를 구성하여 각 클라이언트가 A 레코드를 갱신할 수 있게 해야 합니다. 모든 DHCP 클라이언트가 자신의 A 레코드 갱신 요구 작성을 지원하는 것이 아닙니다. 이 방법을선택하기 전에 클라이언트 플랫폼에 대한 문서를 참조하십시오.

동적 존은 갱신을 송신하는 것이 허용된 권한이 있는 소스 리스트를 작성함으로써 보안이 이루어집니다. 개별 IP 주소, 전체 서브넷, 공유 보안 키(트랜잭션 서명 또는 TSIG라고 함)를 사용한 부호화된 패킷 또는 그와 같은 방법을 조합하여 권한이 있는 소스를 정의할 수 있습니다. DNS는 자원 레코드를 갱신하기 전에 들어오는 요구 패킷이 권한이 있는 소스로부터 오는 것인지를 확인합니다.

동적 갱신은 단일 iSeries 서버에서 DNS와 DHCP 간에, 서로 다른 iSeries 서버 간에 또는 iSeries 서버와 동적 갱신을 수행할 수 있는 기타 서버 간에 수행될 수 있습니다. iSeries용 동적 갱신 구성에 대한 자세한 정보는 다음 주제를 참조하십시오.

- 동적 갱신을 수신하도록 DNS 구성
- 동적 갱신을 송신하도록 DHCP 구성
- DNS로 동적 갱신을 송신하는 서버에는 동적 갱신 API QTOBUPT가 필요합니다. 이것은 OS/400 옵션 31, DNS를 사용하여 자동으로 설치됩니다.

BIND 8 피처

V5R1에서는 DNS가 BIND 8을 사용하도록 재설계되었습니다. PASE를 설치하지 않을 경우 BIND 4.9.3 기반의 이전에 출시된 OS/400 DNS 서버를 구성하여 계속 실행할 수 있습니다. DNS 시스템 요구사항은 iSeries에서 BIND 8 기반의 DNS를 실행할 때 필요한 사항을 설명합니다. 신규 DNS를 사용하면 다음 피처의 장점을 이용할 수 있습니다.

단일 iSeries에서 복수 DNS 서버 실행

이전 릴리스에서는 하나의 DNS 서버만 구성할 수 있었습니다. 이제는 복수 DNS 서버나 인스턴스를 구성할 수 있습니다. 따라서, 서버 간에 논리적 구획을 설정할 수 있습니다. 복수 인스턴스를 작성할 때는 각 인스턴스에 대해 청취 인터페이스 IP 주소를 명시적으로 정의해야 합니다. 두 개의 DNS 인스턴스가 같은 인터페이스에서 청취할 수 없습니다.

복수 서버를 실제로 적용한 실례로 분할 DNS가 있으며, 이 경우에는 하나의 서버를 내부 네트워크용으로 인증하고 다른 서버를 외부 조회에 사용합니다. 분할 DNS에 대한 자세한 내용은 방화벽에서의 분할 DNS를 참조하십시오.

조건부 이송

조건부 이송을 사용할 경우 이송 기본설정을 올바로 설정하기 위해 DNS 서버를 구성할 수 있습니다. 그리고 답을 알 수 없는 모든 조회를 이송하기 위해 서버를 설정할 수 있습니다. 글로벌 레벨에서 이송을 설정할 수

있지만, 정상적인 반복 분석을 강제로 적용할 정의역에는 예외를 추가할 수 있습니다. 또는 글로벌 레벨에서 정상적인 반복 분석을 설정한 다음에 특정 정의역 안으로 강제 이송할 수 있습니다.

안전한 동적 갱신
DHCP 및 기타 권한이 있는 소스는 트랜잭션 서명(TSIG) 및(또는) IP 주소 권한 부여를 사용하여 동적 자원 레코드 갱신을 송신할 수 있습니다. 이렇게 하면 존 자료를 수동으로 갱신할 필요없이 권한이 있는 소스만 갱신에 사용됩니다.

동적 갱신에 대한 자세한 정보는 동적 갱신을 참조하십시오. 외부 소스로부터의 갱신 권한 부여에 대한 자세한 정보는 보안 수단 계획을 참조하십시오.

통지
통지를 작동시키면, 1차 서버에서 존 자료가 갱신될 때마다 DNS 통지 기능이 활성화됩니다. 1차 서버는 알려진 모든 2차 서버로 자료가 변경되었음을 나타내는 메세지를 송신합니다. 그러면 2차 서버가 갱신된 존 자료에 대해 존 전송 요구로 응답합니다. 이렇게 하면 백업 존 자료를 최신 상태로 유지함으로써 2차 서버 지원을 향상시킬 수 있습니다.

존 전송(IXFR 및 AXFR)
이전에는 2차 서버가 존 자료를 다시 로드해야 할 때마다 모든 존 전송(AXFR)에서 전체 자료 세트를 로드해야 했습니다. BIND 8은 신규 존 전송 방법 즉, 존 증분 전송(IXFR)을 지원합니다. IXFR은 다른 서버가 전체 존을 전송하지 않고 변경된 자료만 전송할 수 있는 방법입니다.

1차 서버에서 작동시킬 경우 플래그에 자료 변경이 지정되어 변경이 발생했음을 나타냅니다. 2차 서버가 IXFR에서 존 갱신을 요구하면 1차 서버가 신규 자료만 전송합니다. IXFR은 존이 동적으로 갱신될 때 특히 유용하며, 적은 양의 자료를 전송함으로써 통신 로드를 줄입니다.
주: 이 피처를 사용하기 위해서는 1차 서버와 2차 서버 모두에서 IXFR을 사용할 수 있어야 합니다.

DNS 자원 레코드

DNS 존 데이터베이스는 자원 레코드 콜렉션으로 구성됩니다. 자원 레코드마다 특정 오브젝트에 관한 정보를 지정합니다. 예를 들어, 주소 맵핑(A) 레코드는 호스트명을 IP 주소에 맵핑하고, 역방향 검색 포인터(PTR) 레코드는 IP 주소를 호스트명에 맵핑합니다. 서버는 이 레코드들을 사용하여 그 존에서 호스트 조회에 응답합니다. 자세한 정보는 표에서 DNS 자원 레코드를 보십시오.

<LABEL for=″table″>표에서 레코드를 선택하거나 아래에 단어를 입력하십시오. <LABEL>

———————————————————————————————————-

설명을 보려면 레코드를 선택하십시오.

메일 및 MX 레코드

메일 및 MX 레코드는 단순 우편 전송 프로토콜(SMTP)과 같은 메일 라우팅 프로그램에서 사용됩니다. iSeries DNS가 지원하는 메일 레코드 유형에 대한 자세한 정보는 DNS 자원 레코드에서 검색 표를 참조하십시오.

DNS에는 메일 교환 정보를 사용하는 전자 우편 송신 정보가 들어 있습니다. 네트워크가 DNS를 사용할 경우에는 단순 우편 전송 프로토콜(SMTP) 어플리케이션이 TEST.IBM.COM으로 TCP 연결을 여는 것만으로 TEST.IBM.COM 호스트로 주소 지정된 메일을 전달하지 않습니다. SMTP는 먼저 DNS 서버를 조회하여 메세지 전달에 사용할 수 있는 호스트 서버를 찾습니다.

특정 주소로 메일 전달

DNS 서버는 메일 교환(MX) 레코드라는 자원 레코드를 사용합니다. MX 레코드는 도메인 또는 호스트명을 기본설정 값과 호스트명에 맵핑합니다. 보통은 한 호스트가 다른 호스트를 위한 메일을 처리하도록 지정하기 위해 MX 레코드가 사용됩니다. MX 레코드를 사용하여 첫 번째 호스트에 도달할 수 없을 경우에는 다른 호스트가 메일 전달을 시도하도록 지정할 수 있습니다. 즉, MX 레코드는 한 호스트로 주소 지정된 메일이 다른 호스트로 전달될 수 있게 해줍니다.

동일한 정의역이나 호스트명에 복수 MX 자원 레코드가 있을 수 있습니다. 동일한 정의역이나 호스트에 복수 MX 레코드가 있을 때는 각 레코드의 기본설정(또는 우선순위) 값이 순서(시도할)를 판별합니다. 최하위 기본설정 값이 최우선 레코드에 대응하여 먼저 시도됩니다. 최우선 호스트에 도달할 수 없으면 메일 송신 어플리케이션이 우선 순위가 낮은 다음 MX 호스트에 연결을 시도합니다. 정의역 관리자 또는 MX 레코드 작성자가 기본설정 값을 설정합니다.

DNS 서버 권한에 이름이 있지만 MX가 할당되지 않은 경우에는 DNS 서버가 빈 MX 자원 레코드 리스트로 응답합니다. 이때는 메일 송신 어플리케이션이 목적지 호스트와 직접 연결 설정을 시도합니다. **주:** 도메인 MX 레코드에는 와일드 카드(예: `*.mycompany.com`)를 사용하지 않는 것이 좋습니다.

예: 호스트 MX 레코드

다음 예에서는 기본설정에 따라 시스템이 fsc5.test.ibm.com 메일을 호스트 자체로 전달해야 합니다. 호스트에 도달할 수 없으면, 시스템이 메일을 psfred.test.ibm.com 또는 mvs.test.ibm.com(psfred.test.ibm.com에도 도달할 수 없는 경우)으로 전달합니다. 다음은 이러한 MX 레코드의 예입니다.

```
fsc5.test.ibm.com   IN MX 0 fsc5.test.ibm.com
                       IN MX 2 psfred.test.ibm.com
                       IN MX 4 mvs.test.ibm.com
```

DNS 계획

DNS는 다양한 솔루션을 제공합니다. DNS를 구성하기 전에 네트워크 내에서 어떻게 작동시킬 것인지를 계획하는 것이 중요합니다. DNS를 구현하기 전에 네트워크 구조, 성능, 보안 등의 주제를 검토하십시오. DNS 요구를 계획할 때는 아래의 주제를 고려하십시오.

DNS 권한 판별

DNS 관리자의 경우 특별한 권한 부여 요구사항들이 있습니다. 또한 권한 부여와 관련하여 보안 문제도 고려해야 합니다. 이 주제에서는 그와 같은 요구사항에 관해 설명합니다.

정의역 구조 판별

처음으로 정의역을 설정하는 경우에는 존을 작성하기 전에 요구 및 유지보수 계획을 수립해야 합니다.

보안 수단 계획
DNS는 서버로의 외부 액세스를 제한하는 보안 옵션을 제공합니다. 이 주제에서는 그와 같은 옵션과 액세스 제어 방법에 관해 설명합니다.

DNS 권한 판별

DNS를 설정할 때, 보안 예방책을 강구하여 구성을 보호해야 합니다. 또한 어떤 사용자에게 구성 변경 권한을 부여할 것인지를 설정해야 합니다.

DNS를 구성하고 관리하기 위해서는 iSeries 관리자에게 최소한의 권한 레벨이 필요합니다. 관리자에게 모든 오브젝트에 대한 액세스를 부여하면 관리자가 DNS 관리 타스크를 수행할 수 있습니다. DNS를 구성할 사용자의 경우에는 모든 오브젝트(*ALLOBJ) 권한이 있는 보안 담당자 액세스가 적합합니다. iSeries Navigator를 사용하여 사용자에게 권한을 부여하십시오. 자세한 정보가 필요하면, DNS 온라인 도움말에서 **DNS 관리자에게 권한 부여**를 읽으십시오.

주: 관리자 프로파일에 충분한 권한이 없으면, 모든 DNS 디렉토리 및 관련구성 파일에 대한 권한 및 특정 액세스가 필요합니다.

정의역 구조 판별

정의역 또는 부속 정의역을 존으로 나누는 방법, 네트워크 요구에 최적의 서비스를 제공하는 방법, 인터넷에 액세스하는 방법, 방화벽을 조정하는 방법을 결정하는 것이 중요합니다. 이 요소들은 복잡할 수 있으므로 경우별로 처리해야 합니다. 자세한 지침은 O'Reilly DNS and BIND 책과 같은 권위 있는 소스를 참조하십시오.

DNS 존을 동적 존으로 구성할 경우에는 서버가 실행되는 동안 존 자료를 수동으로 변경할 수 없습니다. 수동으로 변경하면 들어오는 동적 갱신에 방해가 될 수 있습니다. 수동 갱신이 필요하면 서버를 중단하고 변경한 다음에 서버를 재시작하십시오. 중단된 DNS 서버로 송신된 동적 갱신은 절대로 완료되지 않습니다. 이와 같은 이유로 인해 동적 존과 정적 존을 별도로 구성할 수 있습니다. 완전히 분리된 존을 작성하거나 동적으로 유지보수할 그 클라이언트에 대해 dynamic.mycompany.com과 같은 신규 부속 정의역을 정의하여 별도로 구성할 수 있습니다.

iSeries DNS는 서버를 구성하기 위한 그래픽 인터페이스를 제공합니다. 경우에 따라 인터페이스가 다른 소스에서는 달리 표현되는 개념이나 전문 용어를 사용합니다. DNS 구성을 계획할 때 기타 정보 소스를 참조하려면 다음 사항을 기억하는 것이 도움이 될 것입니다.

- 서버에 정의된 모든 존과 오브젝트는 **정방향 검색 존** 폴더와 **역방향 검색 존** 폴더에 구성됩니다. 정방향 검색 존은 정의역명을 A 레코드와 같은 IP 주소에 맵핑하는 데 사용되는 존입니다. 역방향 검색 존은 PTR 레코드와 같은 IP 주소를 정의역명에 맵핑하는 데 사용되는 존입니다.
- iSeries DNS는 **1차 존**과 **2차 존**을 말합니다. 다른 BIND 문서에서는 마스터 존과 종속 존으로 부릅니다.
- 인터페이스는 **서브존**을 사용하는데, 일부 소스에서는 이를 부속 정의역이라고도 합니다. 하위 존은 하나 이상의 이름 서버에 책임을 위임한 서브존입니다.

보안 수단 계획

DNS 서버 보안은 필수적입니다. Information Center에서 IBM Secureway: iSeries및 인터넷을 포함하여 여러 소스에서 다음 보안 고려사항 이외에 DNS 보안 및 iSeries 보안을 다루고 있습니다. DNS 및 BIND 책도 DNS와 관련된 보안 정보를 수록하고 있습니다.

주소 일치 리스트

DNS는 주소 일치 리스트를 사용하여 특정 DNS 기능에 대한 외부 엔티티 액세스를 허용하거나 거부합니다. 이 리스트에는 특정 IP 주소, 서브네트(IP 접두부 사용) 또는 트랜잭션 서명(TSIG) 키 사용이 포함될 수 있습니다. 액세스를 허용하거나 거부할 엔티티 리스트를 주소 일치 리스트에 정의할 수 있습니다. 주소 일치 리스트를 재사용하려는 경우 리스트를 액세스 제어 리스트(ACL)에 저장할 수 있습니다. 그러면 리스트를 제공해야 할 때마다 간단히 ACL을 호출하여 전체 리스트를 로드할 수 있습니다.

주소 일치 리스트 요소 순서

주소가 일치하는 주소 일치 리스트의 첫 번째 요소가 사용됩니다. 예를 들어, 10.1.1.5를 제외한 10.1.1.x 네트워크의 모든 주소를 허용하기 위해서는 일치 리스트 요소의 순서가 반드시 !10.1.1.5; 10.1.1/24이어야 합니다. 이 경우에는 주소 10.1.1.5가 첫 번째 요소와 비교되어 즉시 거부됩니다.

요소가 반전된(10.1.1/24; !10.1.1.5) 경우에는 서버가 일치하는 첫 번째 요소와 비교한 후 나머지 규칙을 검사하지 않기 때문에 IP 주소 10.1.1.5에 액세스가 허용됩니다.

액세스 제어 옵션

DNS를 사용하여 서버로 동적 갱신을 송신할 수 있는 사용자, 자료를 조회할 수 있는 사용자 및 존 전송을 요구할 수 있는 사용자 등의 제한사항을 설정할 수 있습니다. 다음 옵션의 경우 액세스 제어 리스트를 사용하여 서버로의 액세스를 제한할 수 있습니다.

갱신 허용

DNS 서버가 외부 소스로부터 동적 갱신을 허용하게 하려면 갱신 허용 옵션을 작동시켜야 합니다.

조회 허용

이 서버에 조회할 수 있는 호스트를 지정합니다. 지정하지 않은 경우의 디폴트는 모든 호스트로부터 조회를 허용하는 것입니다.

전송 허용

서버로부터 존 전송을 수신할 수 있는 호스트를 지정합니다. 지정하지 않은 경우의 디폴트는 모든 호스트로부터 전송을 허용하는 것입니다.

순환 허용

이 서버를 통해 순환 조회가 허용되는 호스트를 지정합니다. 지정하지 않은 경우의 디폴트는 모든 호스트로부터 순환 조회를 허용하는 것입니다.

블랙홀

서버가 조회를 허용하지 않을 주소 리스트 또는 조회 분석에 사용하지 않을 주소 리스트를 지정합니다. 이 주소로부터의 조회에는 응답하지 않습니다.

DNS 시스템 요구사항

DNS 옵션(옵션 31)은 기본 오퍼레이팅 시스템을 통해 자동으로 설치되는 것이 아닙니다. 설치하려면 DNS를 선택해야 합니다. V5R1에 추가된 신규 DNS 서버는 BIND 8이라는 업계 표준 DNS 구현을 기반으로 하고 있습니다. 이전 OS/400 DNS 서비스는 BIND 4.9.3을 기반으로 한 것이며, V5R1에서도 계속 사용할 수 있습니다.

일단 DNS를 설치한 후에는 디폴트로 이전 릴리스에서 사용할 수 있었던 BIND 4.9.3 기반의 DNS 서버 기능을 사용하여 단일 DNS 서버를 설정하도록 구성이 이루어집니다. BIND 8을 사용하는 하나 이상의 DNS 서버를 실행하려면 PASE(Portable Application Solutions Environment)를 설치해야 합니다. PASE는 SS1 옵션 33입니다. 일단 PASE가 설치되면, iSeries Navigator가 올바른 BIND 구현을 위한 구성을 자동으로 처리합니다.

PASE를 사용하지 않으면, BIND 8 피처의 모든 장점을 이용할 수 없습니다. PASE 없이 BIND 4.9.3을 기반으로 한 DNS 서버를 실행할 수 있습니다. PASE를 사용하지 않더라도 이전 릴리스에서 사용할 수 있었던 BIND 4.9.3을 기반으로 한 동일한 DNS 서버를 실행할 수 있습니다. V4R5 Information Center에서 DNS

를 참조하십시오.

이 DNS 서버로 갱신을 송신하기 위해 서로 다른 iSeries 서버에 DHCP 서버를 구성할 경우 DHCP iSeries에 옵션 31을 설치해야 합니다. DHCP 서버는 옵션 31이 제공하는 프로그래밍 인터페이스를 사용하여 동적 갱신을 수행합니다.

DNS가 설치되어 있는지 알아보려면 다음과 같이 하십시오.

1. 명령행에서 **GO LICPGM**을 입력하고 **Enter**를 누르십시오.
2. **10**(설치된 사용권 프로그램 표시)을 입력하고 **Enter**를 누르십시오.
3. **5722SS1 OS/400 - 정의역명 시스템**(SS1 옵션 31)으로 화면을 이동하십시오.
   DNS가 설치되어 있으면 **설치 상태**가 다음과 같이 ***compatible**입니다.

```
LicPgm     설치 상태           설명
5722SS1    *COMPATIBLE         OS/400 - 정의역명 시스템
```

4. **F3**을 눌러 화면을 나가십시오.

DNS를 설치하려면 다음과 같이 하십시오.

1. 명령행에서 **GO LICPGM**을 입력하고 **Enter**를 누르십시오.
2. **11**(사용권 프로그램 설치)을 입력하고 **Enter**를 누르십시오.
3. OS/400 - 정의역명 시스템 옆의 **옵션** 필드에 **1**(설치)를 입력하고 **Enter**를 누르십시오.
4. 다시 **Enter**를 눌러 설치를 확인하십시오.

DNS 구성

DNS 구성에 대한 작업을 시작하기 전에 DNS 시스템 요구사항을 참조하여 필수 DNS 구성요소를 설치하십시오. 다음의 하위 주제에서는 DNS 서버 구성 지침을 제공합니다.

iSeries Navigator에서 DNS에 액세스
iSeries Navigator에서 DNS에 액세스하기 위한 지침

이름 서버 구성
DNS를 사용하여 복수 이름 서버 인스턴스를 작성할 수 있습니다. 이 주제는 이름 서버 구성 지침을 제공합니다.

동적 갱신을 수신하도록 DNS 구성
다른 소스로부터의 요구를 허용하여 존 자료를 동적으로 갱신하도록 BIND 8을 실행하는 DNS 서버를 구성할 수 있습니다. 이 주제는 DNS 서버가 동적 갱신을 수신할 수 있도록 갱신 허용 옵션을 구성하기 위한 지침을 제공합니다.

DNS 파일 가져오기
DNS는 기존의 존 자료 파일을 가져올 수 있습니다. 기존 구성 파일로부터 신규 존을 작성하려면 다음에 오는 간단한 프로시듀어를 따라 작업하십시오.

외부 DNS 자료에 액세스
DNS 존 자료를 작성할 때 서버가 그 존에 대한 조회를 분석할 수 있습니다. 이 주제에서는 정의역을 벗어난 조회를 분석하기 위한 DNS 구성 방법을 설명합니다.

iSeries Navigator에서 DNS에 액세스

다음은 iSeries Navigator에서 DNS 구성 인터페이스로 안내하는 지침입니다. PASE를 사용할 경우 BIND 8을 기반으로 한 DNS 서버를 구성할 수 있습니다. PASE를 사용하지 않을 경우에는 이전 릴리스에서 사용하던 BIND 4.9.3을 기반으로 한 같은 DNS 서버를 실행할 수 있습니다. V4R5 Information Center에서 BIND 4.9.3을 기반으로 한 DNS 관련 정보 DNS

를 참조하십시오.

처음 DNS를 구성하는 경우 다음과 같이 하십시오.

1. **iSeries Navigator**에서 **사용자 iSeries 서버** —> **Network** —> **서버** —> **DNS**를 확장하십시오.
2. **DNS**를 마우스 오른쪽 버튼으로 클릭한 후 **신규 구성**을 선택하십시오.

V5R1 이전 DNS 서버가 구성되어 있을 경우 다음과 같이 하십시오.

1. **iSeries Navigator**에서 **사용자 iSeries 서버** —> **Network** —> **서버** —> **DNS**를 확장하십시오.
2. 오른쪽 분할 창에서 DNS 서버를 더블 클릭하여 **DNS 구성** 창을 여십시오.

3. PASE를 사용할 경우 기존 DNS 구성을 BIND 8 구현으로 마이그레이트하는 옵션이 제공됩니다. 그러나 일단 BIND 8로 마이그레이트한 후에는 BIND 4.9.3으로 되돌릴 수 없습니다. 확실하지 않으면 **아니오**를 선택하십시오. 그러나 마이그레이션을 원하면 **예**를 선택하십시오.
4. DNS 서버를 BIND 8로 마이그레이트하려면 왼쪽 분할 창에서 **DNS**를 마우스 오른쪽 버튼으로 클릭하고 **버전 8로 마이그레이트**를 선택하십시오.

이름 서버 구성

BIND 8 기반의 iSeries DNS는 복수 이름 서버 인스턴스를 지원합니다. 다음 타스크는 등록 정보 및 존을 포함하여 단일 이름 서버 인스턴스를 작성하는 프로세스로 사용자를 안내합니다.

1. 이름 서버 인스턴스 작성
   신규 DNS 구성 마법사를 사용하여 DNS 서버 인스턴스를 정의합니다.
2. DNS 서버 등록 정보 편집
   신규 서버 인스턴스의 글로벌 등록 정보를 정의합니다.
3. 이름 서버에서 존 구성
   존과 존 자료를 작성하여 이름 서버를 채웁니다.

복수 인스턴스를 작성할 경우 원하는 모든 인스턴스가 작성될 때까지 위에 설명한 프로시듀어를 반복하십시오. 이름 서버 인스턴스별로 디버그 레벨, 자동시작 값과 같은 독립 등록 정보를 지정할 수 있습니다. 신규 인스턴스를 작성할 때 별도로 구성 파일이 작성됩니다. 구성 파일에 관한 자세한 정보는 DNS 구성 파일 유지보수를 참조하십시오.

이름 서버 인스턴스 작성

신규 DNS 구성 마법사를 시작하려면 다음과 같이 하십시오.

1. **iSeries Navigator**에서 **사용자 iSeries 서버** —> **Network** —> **서버** —> **DNS**를 확장하십시오.
2. 왼쪽 분할 창에서 **DNS**를 오른쪽 마우스 버튼으로 클릭하고 **신규 이름 서버...**를 선택하십시오.
3. 마법사가 구성 프로세스로 사용자를 안내합니다.

마법사가 다음 입력을 요구합니다.

DNS 서버명: DNS 서버명을 입력하십시오. 서버명은 최대 5자까지 가능하며, 영문자로 시작해야 합니다. 복수 서버를 작성하는 경우 각 서버에는 고유명이 있어야 합니다. 이 이름을 다른 시스템 영역에서는 DNS 서버 ″인스턴스″ 이름이라고 합니다.

청취 IP 주소: 두 개의 DNS 서버가 같은 IP 주소를 청취할 수는 없습니다. 디폴트 설정 값은 모든 IP 주소를 청취하는 것입니다. 서버 인스턴스를 추가로 작성할 경우에소 모두(ALL)에서 청취하도록 구성할 수 없습니다. 반드시 서버마다 IP 주소를 지정해야 합니다.

루트 서버: 디폴트 인터넷 루트 서버 리스트를 로드하거나 인트라넷용 내부 루트 서버와 같은 자신의 루트 서버를 지정할 수 있습니다.
주: 인터넷에 연결되어 있고 DNS가 인터넷명을 완전히 분석할 수 있을 것으로 예상하는 경우에는 디폴트 인터넷 루트 서버만 로드하십시오.

서버 시작: TCP/IP가 시작될 때 서버가 자동으로 시작되어야 하는지를 지정할 수 있습니다. 복수 서버를 작동시킬 때, 다른 인스턴스와 관계없이 인스턴스를 개별적으로 시작하고 종료할 수 있습니다.

다음에 할 일: DNS 서버 등록 정보 편집

DNS 서버 등록 정보 편집

이름 서버를 작성한 후에는 갱신 허용 및 디버그 레벨과 같은 등록 정보를 편집할 수 있습니다. 이 옵션들은 변경 중인 서버 인스턴스에만 적용됩니다. DNS 서버 인스턴스의 등록 정보를 편집하려면 다음과 같이 하십시오.

1. **iSeries Navigator**에서 **사용자 iSeries 서버** —> **Network** —> **서버** —> **DNS**를 확장하십시오.
2. 오른쪽 분할 창에서 **사용자 DNS 서버**를 오른쪽 마우스 버튼으로 클릭하고 **구성**을 선택하십시오.
3. **DNS 서버**를 오른쪽 마우스 버튼으로 클릭하고 **등록 정보**를 선택하십시오.

다음에 할 일: 이름 서버에서 존 구성

이름 서버에서 존 구성

일단 이름 서버를 작성했으면, **iSeries Navigator** 기본 창으로 돌아가십시오. 오른쪽 분할 창에 사용자 서버가 표시됩니다. 서버에서 존을 구성하려면 서버명을 오른쪽 마우스 버튼으로 클릭하고 **구성**을 선택하십시오. **DNS 구성** 창이 표시됩니다.

모든 존은 마법사를 사용하여 구성됩니다. 해당 폴더를 오른쪽 마우스 버튼으로 클릭하여 **정방향 검색 존** 또는 **역방향 검색 존**을 작성하십시오. 그 존 유형에 사용할 수 있는 옵션이 표시됩니다. 작성할 존 유형을 선택하여 마법사를 시작하십시오.

V5R1 DNS에서 작성할 수 있는 오브젝트 유형의 설명은 DNS 이해를 참조하십시오.

일단 존을 구성했으면, 자세한 구성 정보를 위해 다음 주제를 참조할 수 있습니다.

동적 갱신을 허용하도록 존 구성
동적 갱신은 권한이 있는 소스가 존 자료를 갱신하기 위해 자원 레코드를 송신할 수 있게 합니다. 이렇게 하면 수동으로 존 자료를 변경해야 하는 경우가 줄어듭니다.

존 자료 가져오기
다른 DNS 서버에서 온 기존의 존 자료 파일이 있으면, 이 파일을 신규 서버로 업로드할 수 있습니다.

외부 DNS 자료에 액세스
서버에 포함된 존 자료를 벗어난 정보에 대한 조회를 분석할 수 있도록 서버를 구성할 수 있습니다. 인증된 다른 서버로 조회를 이송하거나 루트 서버를 로드하여 조회를 분석할 수 있습니다.

동적 갱신을 수신하도록 DNS 구성

동적 존을 작성할 때는 네트워크 구조를 고려해야 합니다. 정의역의 일부를 여전히 수동으로 갱신해야 할 경우에는 정적 존 및 동적 존을 별도로 설정할 것을 고려해야 합니다. 동적 존을 수동으로 갱신하기 위해서는 동적 존 서버를 중단한 후 갱신이 완료되면 다시 시작해야 합니다. 서버를 중단하면 서버가 존 데이터베이스에서 존

자료를 로드한 이후로 갱신된 모든 동적 갱신을 동기화시킵니다. 서버를 중단시키지 않으면 서버가 시작된 이후로 처리된 모든 동적 갱신이 유실됩니다. 그러나 수동으로 갱신하기 위해 서버를 중단하는 것은 서버가 중단되었을 때 송신된 동적 갱신이 이루어지지 않을 수 있다는 것을 나타냅니다.

DNS는 오브젝트가 갱신 허용 명령문에 정의되어 있을 때 존이 동적 존임을 나타냅니다. 갱신 허용 옵션을 구성하려면 다음과 같이 하십시오.

1. **iSeries Navigator**에서 **사용자 iSeries 서버** —> **Network** —> **서버** —> **DNS**를 확장하십시오.
2. 오른쪽 분할 창에서 **사용자 DNS 서버**를 오른쪽 마우스 버튼으로 클릭하고 **구성**을 선택하십시오.
3. **DNS 구성** 창에서 **정방향 검색 존** 또는 **역방향 검색 존**을 확장하십시오.
4. 편집할 1차 존을 오른쪽 마우스 버튼으로 누르고 **등록 정보**를 선택하십시오.
5. **1차 존 등록 정보** 페이지에서 **옵션** 탭을 클릭하십시오.
6. **옵션** 페이지에서 **액세스 제어** —> **갱신 허용**을 확장하십시오.
7. DNS는 주소 일치 리스트를 사용하여 권한이 있는 갱신을 확인합니다. 주소 일치 리스트에 오브젝트를 추가하려면 주소 일치 리스트 요소 유형을 선택하고 **추가...**를 클릭하십시오. IP 주소, IP 접두부, 액세스 제어 리스트 또는 키를 추가할 수 있습니다.
8. 주소 일치 리스트 갱신을 완료했으면, **확인**을 눌러 **옵션** 페이지를 닫으십시오.

iSeries DHCP 서버로부터 동적 갱신을 수신하도록 DNS를 설정하려면 동적 갱신을 송신하도록 DHCP 구성을 참조하십시오.

DNS 파일 가져오기

존 자료 파일을 가져오거나 기존 호스트 표를 변환하여 1차 존을 작성할 수 있습니다. 호스트 표에서 존 자료를 작성하려면 V4R5 Information Center에서 호스트 표 변환

을 참조하십시오.

BIND 구문을 기반으로 한 유효한 존 구성 파일을 가져올 수 있습니다. IFS 디렉토리에 파일이 있어야 합니다. 파일 가져오기를 마치면 DNS가 유효한 존 자료 파일인지 확인한 후에 이 서버 인스턴스의 NAMED.CONF 파일에 추가합니다.

존 파일을 가져오려면 다음과 같이 하십시오.

1. **iSeries Navigator**에서 **사용자 iSeries 서버** —> **Network** —> **서버** —> **DNS**를 확장하십시오.
2. 오른쪽 분할 창에서 존을 가져올 DNS 서버 인스턴스를 더블 클릭하십시오.
3. 왼쪽 분할 창에서 **DNS 서버**를 마우스 오른쪽 버튼으로 클릭한 후 **존 가져오기**를 선택하십시오.
4. 1차 존을 가져오려면 마법사의 지침에 따라 작업하십시오.

레코드 유효성

정의역 자료 가져오기 기능은 가져오는 파일의 각 레코드를 읽고 유효성을 검사합니다. 정의역 자료 가져오기 기능이 완료되면 가져온 존의 **기타 레코드** 등록 정보 페이지에서 개별적으로 오류 레코드를 검사합니다.

- **주:**
- 대형 1차 정의역을 가져오려면 4-5분 정도가 소요됩니다.
- 정의역 자료 가져오기 기능은 $include 지시문을 지원하지 않습니다. 가져오기 정의역 자료의 유효성 검사 프로세스가 $include 지시문에 오류가 있는 행을 식별합니다.

외부 DNS 자료에 액세스

루트 서버는 인터넷이나 대형 인트라넷에 직접 연결된 DNS 서버 기능에 중요합니다. DNS 서버가 자신의 정의역 파일에 포함된 조회가 아닌 호스트에 대한 조회에 응답할 때는 반드시 루트 서버를 사용해야 합니다.

자세한 정보를 구하기 위해서는 DNS 서버가 검색 위치를 알아야 합니다. 인터넷에서는 DNS 서버가 검색하는 첫 번째 위치가 루트 서버입니다. 루트 서버는 응답을 찾을 때까지 또는 응답이 없다는 사실을 알 때까지 그 계층 안의 다른 서버로 DNS 서버를 지시합니다.

iSeries Navigator의 디폴트 루트 서버 리스트

인터넷에 연결되어 있으며, DNS 서버에서 이름이 분석되지 않아서 인터넷에서 이름을 분석하려는 경우에만 인터넷 루트 서버를 사용해야 합니다. iSeries Navigator가 인터넷 루트 서버의 디폴트 리스트를 제공합니다. 이 리스트는 iSeries Navigator가 릴리스될 때 최신 리스트로 제공됩니다. 디폴트 리스트가 최신 리스트인지 확인하려면 디폴트 리스트를 InterNIC 사이트의 리스트와 비교하십시오. 사용자 구성의 루트 서버 리스트를 갱신하여 최신 정보로 유지하십시오.

인터넷 루트 서버 주소 확보 위치

최상위 레벨 루트 서버의 주소는 수시로 변하므로 DNS 관리자가 최신 정보로 유지시켜야 합니다. InterNIC가 인터넷 루트 서버 주소 리스트를 최신 정보로 유지하고 있습니다. 인터넷 루트 서버의 최신 리스트를 얻으려면 다음과 같이 하십시오.

1. InterNIC 서버에 Anonymous FTP를 시작합니다.`FTP.RS.INTERNIC.NET`
2. 파일을 다운로드합니다. `/domain/named.root`
3. 디렉토리에 파일을 저장합니다. `Integrated File System/Root/QIBM/ProdData/OS400/DNS/ROOT.FILE`.

방화벽 뒤의 DNS 서버에는 루트 서버가 정의되어 있지 않을 수 있습니다. 이 경우 DNS 서버가 자신의 1차 정의역 데이터베이스 파일이나 캐시에 있는 항목에서만 조회를 분석할 수 있습니다. 또는 방화벽 DNS로 오프사이트 조회를 이송할 수도 있습니다. 이 경우 방화벽 DNS 서버가 이송자의 역할을 합니다.

인트라넷 루트 서버

DNS 서버가 대형 인트라넷의 한 부분이면 루트 서버를 가질 수 있습니다. DNS 서버가 인터넷에 액세스하지 않을 경우에는 디폴트 인터넷 서버를 로드하지 않아도 됩니다. 그러나 DNS 서버가 정의역을 벗어나 내부 주소를 분석하도록 하기 위해서는 내부 루트 서버를 추가해야 합니다.

DNS 관리

DNS를 구성했으면, 다음 주제를 검토하십시오.

NSLookup을 사용하여 DNS 기능 확인
NSlookup을 사용하여 DNS가 작동하는지 확인할 수 있습니다.

보안 키 관리
보안 키를 사용하여 DNS 자료에 대한 액세스를 제한할 수 있습니다.

DNS 서버 통계
데이터베이스 덤프 및 통계 툴이 서버 성능을 검토하고 관리하는 것을 도와줍니다.

DNS 구성 파일 유지보수
DNS가 사용하는 파일을 이해하고, 파일 백업 및 유지보수를 위한 지침을 검토하십시오.

확장 DNS 옵션
이 주제에서는 사용 경험이 많은 관리자들이 확장 기능에 액세스할 수 있는 방법에 관해 설명합니다.

NSlookup을 사용하여 DNS 기능 확인

IP 주소에 대한 DNS 서버를 조회하려면 NSLookup(Name Server Lookup)을 사용하십시오. 이것은 DNS 서버가 조회에 응답하고 있는지 확인합니다. loopback IP 주소(127.0.0.1)와 연관된 호스트명을 요구하십시오. 호스트명(localhost)으로 응답해야 합니다. 확인하려는 서버 인스턴스에 정의된 특정 이름도 조회해야 합니다. 이렇게 하면 테스트 중인 특정 서버 인스턴스가 올바로 기능하는지 알 수 있습니다.

NSlookup을 사용하여 DNS 기능을 확인하려면 다음과 같이 하십시오.

1. 명령행에서 NSLOOKUP DMNNAMSVR(n.n.n.n)을 입력하십시오. 여기서, n.n.n.n은 청취 테스트를 위해 서버 인스턴스를 구성한 주소입니다.
2. 명령행에서 NSLOOKUP을 입력하고 **Enter**를 누르십시오. NSlookup 조회 세션이 시작됩니다.
3. 서버명 앞에 server를 입력하고 **Enter**를 누르십시오(예: server myiseries.mycompany.com). 다음 정보가 표시됩니다.

   ```
   서버:  myiseries.mycompany.com
   주소: n.n.n.n
   ```

   여기서, n.n.n.n은 DNS 서버의 IP 주소를 나타냅니다.
4. 명령행에서 127.0.0.1을 입력하고 **Enter**를 누르십시오.

   loopback 호스트명을 포함하여 다음 정보를 표시해야 합니다.

   ```
    > 127.0.0.1  서버:  myiseries.mycompany.com
   주소: n.n.n.n

   이름:    localhost
   주소:  127.0.0.1
   ```

   localhost가 리턴될 경우 DNS 서버가 올바로 응답하는 것입니다.

5. exit를 입력하고 **Enter**를 눌러 NSLOOKUP 단말기 세션을 종료하십시오.

주: NSlookup을 사용할 때 도움말이 필요하면 ?을 입력하고 **Enter**를 누르십시오.

보안 키 관리

DNS와 관련하여 두 가지 유형의 키가 있습니다. 키마다 DNS 구성을 보안할 때 서로 다른 역할을 합니다. 다음 설명은 각 유형이 DNS 서버와 어떻게 관련되어 있는지를 설명한 것입니다.

DNS 키

DNS 키는 BIND를 위해 정의된 키입니다. 이 키는 들어오는 갱신을 확인하는 처리의 한 부분으로 DNS 서버가 사용하는 것입니다. 키를 구성하여 이름을 지정할 수 있습니다. 이와 같이 하면 동적 존과 같은 DNS 오브젝트를 보호하려는 경우에 주소 일치 리스트에 키를 지정할 수 있습니다.

DNS 키를 관리하려면 다음과 같이 하십시오.

1. **iSeries Navigator**에서 **사용자 iSeries 서버** —> **Network** —> **서버** —> **DNS**를 확장하십시오.
2. 오른쪽 분할 창에서 열려고 하는 DNS 서버 인스턴스를 오른쪽 마우스 버튼으로 클릭하고 **구성**을 선택하십시오.
3. **DNS 구성** 창에서 **파일** > **키 관리...**를 선택하십시오.

동적 갱신 키

동적 갱신 키는 DHCP 서버가 동적 갱신을 보안하는 데 사용됩니다. 이 키는 DNS와 DHCP가 동일한 iSeries에 있으면 반드시 있어야 합니다. DHCP가 서로 다른 iSeries에 있으면, 동적 갱신을 보안할 수 있도록 각 iSeries 서버에 동일한 동적 갱신 키를 작성해야 합니다.

동적 갱신 키를 관리하려면 다음과 같이 하십시오.

1. **iSeries Navigator**에서 **사용자 iSeries 서버** —> **Network** —> **서버** —> **DNS**를 확장하십시오.
2. **DNS**를 오른쪽 마우스 버튼으로 클릭하고 **동적 갱신 키 관리...**를 선택하십시오.

DNS 서버 통계

DNS는 여러 가지 진단 툴을 제공합니다. 서버 성능을 모니터하는 데 이 툴을 사용할 수 있습니다.

서버 통계

DNS를 사용하여 서버 인스턴스 통계를 볼 수 있습니다. 이 통계는 서버가 마지막으로 재시작되거나 데이터베이스를 다시 로드한 이후로 서버가 수신한 조회 및 응답 수를 정리한 것입니다. 파일을 삭제할 때까지 이 파일에 계속해서 정보가 추가됩니다. 이 정보는 서버가 수신하는 통신량을 평가하고 문제점을 추적하는 데 유용합니다. 서버 통계에 대한 자세한 정보는 DNS 온라인 도움말 주제, **DNS 서버 통계 이해**를 참조하십시오.

서버 통계에 액세스하려면 다음과 같이 하십시오.

1. **iSeries Navigator**에서 **사용자 iSeries 서버** —> **Network** —> **서버** —> **DNS**를 확장하십시오.
2. 오른쪽 분할 창에서 **사용자 DNS 서버**를 오른쪽 마우스 버튼으로 클릭하고 **구성**을 선택하십시오.
3. **DNS 구성** 창에서 **보기** —> **서버 통계**를 선택하십시오.

활동 서버 데이터베이스

DNS를 사용하여 인증 자료, 캐시 자료, 서버 인스턴스에 대한 추가 정보 자료 덤프를 볼 수 있습니다. 덤프에는 서버가 조회로부터 구한 정보 뿐만 아니라 서버의 1차 존 및 2차 존(정방향 및 역방향 맵핑 존)의 정보가 들어 있습니다. 데이터베이스에는 권한 시작(SOA) 정보와 같은 일부 존 등록 정보, 메일 교환(MX) 정보와 같은 호스트 등록 정보를 포함하여 존 및 호스트 정보가 들어 있습니다. 이 정보는 문제점을 추적하는 데 유용합니다.

iSeries Navigator를 사용하여 활동 서버 데이터베이스 덤프를 볼 수 있습니다. 파일 사본을 저장해야 할 경우 데이터베이스 덤프 파일명은 iSeries 디렉토리 경로 **Integrated File System/Root/QIBM/UserData/OS400/DNS/<server instance>**에서 NAMED_DUMP.DB입니다. 여기서, "<server instance>"는 DNS 서버 인스턴스명입니다. 활동 서버 데이터베이스에 대한 자세한 정보는 DNS 온라인 도움말 주제 **DNS 서버 데이터베이스 덤프 이해**에서 구할 수 있습니다.

활동 서버 데이터베이스 덤프에 액세스하려면 다음과 같이 하십시오.

1. **iSeries Navigator**에서 **사용자 iSeries 서버** —> **Network** —> **서버** —> **DNS**를 확장하십시오.
2. 오른쪽 분할 창에서 **사용자 DNS 서버**를 오른쪽 마우스 버튼으로 클릭하고 **구성**을 선택하십시오.
3. **DNS 구성** 창에서 **보기** —> **활동 서버 데이터베이스**를 선택하십시오.

DNS 구성 파일 유지보수

OS/400 DNS를 사용하여 iSeries에서 DNS 서버 인스턴스를 작성하고 관리할 수 있습니다. DNS 구성 파일은 iSeries Navigator에서 관리합니다. 수동으로 파일을 편집해서는 안됩니다. 항상 iSeries Navigator를 사용하여 DNS 구성 파일을 작성, 변경 또는 삭제하십시오. DNS 구성 파일은 아래 나오는 통합 파일 시스템 경로에 저장됩니다.

주: 다음 파일 구조는 BIND 8에서 실행되는 DNS에 적용됩니다. BIND 4.9.3을 기반으로 한 DNS를 사용할 경우에는 V4R5 DNS Information Center 주제에서 DNS 구성 파일 백업 및 기록부 파일 유지보수

를 참조하십시오.

다음 표에서 각 파일들은 표시된 계층 경로에 나열됩니다. 저장 아이콘

이 있는 파일을 백업하여 자료를 보호해야 합니다. 삭제 아이콘

이 있는 파일은 정기적으로 삭제시켜야 합니다.

이름		설명
QIBM/UserData/OS400/DNS/		DNS 시작 디렉토리

이름		설명
ATTRIBUTES		DNS는 이 파일을 사용하여 현재 사용 중인 BIND 버전을 판별합니다.
QIBM/UserData/OS400/DNS/<*instance-n*>/		DNS 인스턴스 시작 디렉토리
ATTRIBUTES		iSeries DNS에서 사용되는 구성 속성
NAMED.CONF		이 파일에는 구성 정보가 들어 있습니다. 관리 중인 특정 존, 존 파일 위치, 동적으로 갱신가능한 존, 이송 서버 위치, 기타 옵션 설정을 서버에 알리기 위해 사용됩니다.
BOOT.AS400BIND4		이 인스턴스에 대해 BIND 8 NAMED.CONF 파일로 변환된 BIND 4.9.3 서버 구성 및 정책 파일. 이 파일은 BIND 4.9.3 서버에서 BIND 8로 마이그레이트하는 경우에 작성됩니다. 마이그레이션을 위한 백업 서비스를 제공하며, BIND 8 서버가 올바로 작동할 때 삭제시킬 수 있습니다.
NAMED.CA		이 서버 인스턴스에 대한 루트 서버 리스트
NAMED_DUMP.DB		활동 서버 데이터베이스에 대해 작성된 서버 자료 덤프
NAMED.STATS		서버 통계
NAMED.PID		실행 중인 서버의 프로세스 ID를 보유합니다. 이 파일은 DNS 서버가 시작할 때마다 작성됩니다. 데이터베이스, 통계, 서버 갱신 기능에 사용됩니다. 이 파일을 삭제하거나 편집하지 마십시오.
QUERYLOG		수신된 조회에 대한 DNS 서버 기록부. DNS 서버 기록부가 활동할 때 파일이 작성됩니다. 서버 기록부가 활동을 시작하면 이 파일 크기가 커지므로 정기적으로 삭제해야 합니다.
<*zone-name-a*>.DB		이 서버가 제공할 특정 정의역에 대한 존 파일. 이 존에 대한 모든 자원 레코드가 들어 있습니다.
<*zone-name-b*>.DB		이 서버가 제공할 특정 정의역에 대한 존 파일. 이 존에 대한 모든 자원 레코드가 들어 있습니다. 각 존에는 별도의 .DB 파일이 있습니다.

이름		설명
.ixfr.		존 증분 전송(IXFR) 파일. 2차 서버는 이 파일을 사용하여 마지막으로 존 전송이 이루어진 이후로 변경된 자료만 로드합니다. 갱신이 발생할 때마다 IXFR 파일 수가 증가합니다. 이전 IXFR 파일은 정기적으로 삭제시켜야 합니다. 하루나 이틀 안에 작성된 파일들을 그대로 두면 대부분의 2차 서버가 IXFR을 로드합니다. 모든 파일을 삭제하면 2차 서버가 전체 전송(AXFR)을 요구합니다.
TMP		임시 작업 파일을 작성하기 위해 서버 인스턴스가 사용하는 디렉토리
QIBM/UserData/OS400/DNS/TMP		나중에 iSeries Navigator를 사용하여 가져오기할 호스트 표에서 덤프된 중간 파일을 작성하기 위해 QTOBH2N 프로그램이 사용하는 임시 디렉토리
QIBM/UserData/OS400/DNS/_DYN/		동적 갱신에 필요한 파일을 보유하고 있는 디렉토리
<*key_id-name-x*>._KID		key_id named <*key_id-name-x*>에 대한 BIND 8 키 명령문이 들어 있는 파일
<*key_id-name-x*>._DUK.<*zone-name-a*>		<*key_id-name-x*> 키를 사용하여 <*zone-name-a*>에 대한 동적 갱신 요구를 초기화하는 데 필요한 동적 갱신 키
<*key_id-name-y*>._KID		key_id named <*key_id-name-y*>에 대한 BIND 8 키 명령문이 들어 있는 파일
<*key_id-name-y*>._DUK.<*zone-name-a*>		<*key_id-name-y*> 키를 사용하여 <*zone-name-a*>에 대한 동적 갱신 요구를 초기화하는 데 필요한 동적 갱신 키
<*key_id-name-y*>._DUK.<*zone-name-b*>		<*key_id-name-y*> 키를 사용하여 <*zone-name-b*>에 대한 동적 갱신 요구를 초기화하는 데 필요한 동적 갱신 키

확장 DNS 피처

iSeries Navigator의 DNS는 DNS 서버를 구성하고 관리하기 위한 인터페이스를 제공합니다. iSeries 그래픽 인터페이스에 익숙한 관리자들을 위해 다음 타스크들을 단축키로 제공합니다. 복수 인스턴스의 서버 상태와 속성을 한번에 변경하는 빠른 방법을 제공합니다.

DNS 속성 변경

DNS 인터페이스를 사용하여 서버 인스턴스 자동시작 및 디버그 레벨을 모두 한번에 변경할 수는 없습니다. 문자 기반의 인터페이스를 사용하여 개별 DNS 서버 인스턴스의 설정 값을 변경하거나 모든 인스턴스의 설정 값을 동시에 변경할 수 있습니다. CHGDNSA를 사용하려면 다음의 단계를 수행하십시오.

1. 명령행에서 CHGDNSA를 입력하고 **F4**를 누르십시오.
2. CHGDNSA(DNS 서버 속성 변경) 페이지에서 단일 서버 인스턴스명을 입력하거나 *ALL을 입력하고 **Enter**를 누르십시오.

사용할 수 있는 서버 속성 옵션이 표시됩니다.

```
서버 자동시작 . . . . . . . . . *SAME *YES, *NO, *SAME
디버그 레벨 . . . . . . . . . . *SAME 0-11, *SAME, *DFT
```

3. **자동시작** TCP/IP가 시작될 때 선택된 DNS 서버가 자동으로 시작되도록 지정하려면 *YES를 입력하십시오. TCP/IP가 시작될 때 서버가 시작되지 않도록 하려면 *NO를 입력하십시오. 현재 속성 설정 값을 그대로 유지하려면 *SAME을 입력하십시오.

   디버그 레벨 선택된 DNS 서버가 사용할 디버그 레벨을 변경하려면 0-11 값을 입력하십시오. 디버그 레벨이 서버 시작 디버그 값을 계승하도록 지정하려면 *DFT를 입력하십시오. 현재 속성 설정 값을 그대로 유지하려면 *SAME을 입력하십시오.

   모든 기본설정을 완료했으면, **Enter**를 눌러 DNS 속성을 설정하십시오.

DNS 서버 시작 또는 중단

DNS 인터페이스를 사용하여 복수 서버 인스턴스를 한번에 시작하거나 중단할 수는 없습니다. 복수 인스턴스 설정 값을 한번에 변경하기 위해서는 문자 기반의 인터페이스를 사용할 수 있습니다. 문자 기반의 인터페이스를 사용하여 모든 DNS 서버 인스턴스를 한번에 시작하려면 명령행에서 STRTCPSVR SERVER(*DNS) DNSSVR(*ALL)을 입력하십시오. 모든 DNS 서버를 한번에 중단하려면 명령행에 ENDTCPSVR SERVER(*DNS) DNSSVR(*ALL)을 입력하십시오.

디버그 값 변경

iSeries Navigator의 DNS 인터페이스는 서버가 실행되는 동안 디버그 레벨을 변경할 수 없습니다. 그러나 문자 기반의 인터페이스를 사용할 경우 서버가 실행되는 동안 디버그 레벨을 변경할 수 있습니다. 이 피처는 대형 존을 사용하며 서버가 처음 시작되어 모든 존 자료를 로드하는 동안 많은 양의 디버그 자료를 받지 않으려는 관리자에게 유용합니다. 문자 기반의 인터페이스를 사용하여 디버그 레벨을 변경하려면 다음과 같이 <instance>를 서버 인스턴스명으로 대체하십시오.

1. 명령행에 ADDLIBLE QDNS를 입력하고 **Enter**를 누르십시오.
2. 디버그 레벨을 변경하십시오.
   - 디버깅을 작동시키거나 디버그 레벨을 하나씩 증가시키려면 CALL QTOBDRVS ('BUMP' '<instance>')를 입력하고 **Enter**를 누르십시오.
   - 디버깅을 작동시키지 않으려면 CALL QTOBDRVS ('OFF' '<instance>')를 입력하고 **Enter**를 누르십시오.

DNS 문제 해결

DNS는 다른 TCP/IP 기능 및 어플리케이션과 마찬가지로 작동합니다. SMTP나 FTP 어플리케이션처럼 DNS 작업도 QSYSWRK 서브시스템에서 실행되며, DNS 작업과 연관된 정보가 있는 사용자 프로파일 QTCP 밑에 작업 기록부를 생성합니다. DNS 작업이 중단되면, 작업 기록부를 사용하여 원인을 판별할 수 있습니다. DNS 서버가 예상한 응답을 리턴하지 않을 경우 작업 기록부에서 문제점 분석에 도움이 되는 정보를 참조할 수 있습니다.

DNS 구성은 여러 개의 파일로 구성되는데, 파일별로 서로 다른 여러 가지의 레코드 유형이 있습니다. DNS 서버에 발생하는 문제점은 일반적으로 DNS 구성 파일에 틀린 항목이 있기 때문입니다. 문제가 발생하면, DNS 구성 파일에 자신이 예상한 항목이 있는지 확인하십시오.

기록
DNS는 사용자가 문제의 원인을 찾으려 할 때 조정을 통해 문제를 해결하는 데 도움을 주는 많은 기록 옵션을 제공합니다. 기록은 다양한 심각도 레벨, 메세지 범주, 출력 파일을 제공함으로써 문제점을 찾는 데 도움이 되도록 기록을 세밀하게 조정할 수 있는 유연성을 제공합니다.

디버그 설정
DNS는 12가지의 디버그 제어 레벨을 제공합니다. 일반적으로 기록을 통해 문제점을 찾기 위한 더 쉬운 방법을 제공받을 수 있으나 디버깅이 필요한 경우도 있습니다. 정상적인 조건 하에서는 디버깅이 작동되지 않습니다(값 = 0).

기타 문제 해결 자원
일반적인 DNS 문제 해결 정보는 여러 가지 소스를 통해 입수할 수 있습니다. 특히, O'Reilly DNS and BIND 책을 일반적인 질문에 대한 좋은 참조서로 사용할 수 있으며, DNS 자원 디렉토리를 통해 DNS 관리자를 위한 토론 그룹으로의 링크를 구할 수 있습니다.

작업 식별
DNS 서버 기능(예: WRKACTJOB 사용)을 확인하기 위해 작업 기록부를 검색하려면 다음의 명명 지침을 고려하십시오.

- BIND 4.9.3을 사용하는 경우 서버 작업명은 QTOBDNS입니다. DNS 4.9.3 디버깅에 대한 자세한 정보는 V4R5 TCP/IP Configuration and Reference

  에서 DNS 문제 해결을 참조하십시오.
- BIND 8 기반의 서버를 실행하는 경우 실행 중인 각 서버 인스턴스에 대한 별도의 작업이 있습니다. 작업명은 5자로 고정되어 있으며(QTOBD), 그 뒤에 인스턴스명이 옵니다. 예를 들어, 두 개의 인스턴스 INST1과 INST2가 있을 경우의 작업명은 QTOBDINST1과 QTOBDINST2입니다.

DNS 서버 기록

BIND 8은 여러 가지 새로운 기록 옵션을 제공합니다. 기록되는 메세지 유형, 각 메세지 유형이 송신되는 위치, 기록할 각 메세지 유형의 심각도를 지정할 수 있습니다. 일반적으로 디폴트 기록 설정 값을 그대로 사용하는 것이 좋지만 변경해야 할 경우 BIND 8 문서의 다른 소스들을 참조하십시오.

기록 채널
DNS 서버는 서로 다른 출력 채널에 메세지를 기록할 수 있습니다. 채널이 기록 자료가 송신되는 위치를 지정합니다. 다음의 채널 유형을 선택할 수 있습니다.

- **파일 채널**
  파일 채널에 기록된 메세지는 파일로 송신됩니다. 디폴트 파일 채널은 as400_debug 및 as400_QPRINT입

니다. 디폴트로 디버그 메세지는 NAMED.RUN 파일인 as400_debug 채널에 기록되지만 이 파일로 기타 메세지 범주가 송신되도록 지정할 수 있습니다. as400_QPRINT에 기록된 메세지 범주들은 사용자 프로파일 QTCP를 위한 QPRINT 스풀 파일로 송신됩니다. 제공되는 디폴트 채널 외에 고유 파일 채널을 작성할 수 있습니다.

- **Syslog 채널**
  이 채널에 기록된 메세지는 서버 작업 기록부로 송신됩니다. 디폴트 syslog 채널은 as400_joblog입니다. 이 채널로 라우트된 기록 메세지는 DNS 서버 인스턴스의 작업 기록부로 송신됩니다.
- **널(null) 채널**
  널 채널에 기록된 모든 메세지는 삭제됩니다. 디폴트 널 채널은 as400_null입니다. 기록부 파일에 메세지가 나타나지 않도록 하려면 범주를 널 채널로 라우트할 수 있습니다.

메세지 범주

메세지는 범주로 그룹화됩니다. 각 채널에 기록되어야 하는 메세지 범주를 지정할 수 있습니다. 다음을 포함하여 여러 가지 범주가 있습니다.

- config: 구성 파일 처리
- db: 데이터베이스 조작
- queries: 서버가 수신하는 모든 조회에 대해 간단한 기록부 메세지 생성
- lame-servers: 잘못된 위임 감지
- update: 동적 갱신
- xfer-in: 서버가 수신하는 존 전송
- xfer-out: 서버가 송신하는 존 전송

기록부 파일 파일 크기가 커질 수 있으므로 정기적으로 삭제시켜야 합니다. 모든 DNS 서버 기록부 파일 내용은 DNS 서버를 중단했다가 다시 시작할 때 지워집니다.

메세지 심각도

채널을 사용하여 메세지 심각도를 필터링할 수 있습니다. 채널별로 메세지가 기록되는 심각도 레벨을 지정할 수 있습니다. 사용할 수 있는 심각도 레벨은 다음과 같습니다.

- Critical
- Error
- Warning
- Notice
- Info
- Debug(디버그 레벨 0-11 지정)
- Dynamic(서버 시작 디버그 레벨 계승)

선택한 심각도의 모든 메세지와 리스트에서 그 위에 있는 레벨이 모두 기록됩니다. 예를 들어, Warning을 선택하면 채널이 Warning, Error, Critical 메세지를 기록합니다. Debug 레벨을 선택하면, 기록될 디버그 메세지에 0-11 값을 지정할 수 있습니다.

기록 설정 값 변경

기록 옵션에 액세스하려면 다음과 같이 하십시오.

1. **iSeries Navigator**에서 **사용자 iSeries 서버** —> **Network** —> **서버** —> **DNS**를 확장하십시오.
2. 오른쪽 분할 창에서 **사용자 DNS 서버**를 오른쪽 마우스 버튼으로 클릭하고 **구성**을 선택하십시오.
3. **DNS 구성** 창에서 **DNS 서버**를 오른쪽 마우스 버튼으로 클릭하고 **등록 정보**를 선택하십시오.
4. **서버 등록 정보** 창에서 **채널** 탭을 선택하여 신규 파일 채널이나 채널 등록 정보(예: 각 채널에 기록된 메세지 심각도)를 작성하십시오.
5. **서버 등록 정보** 창에서 **기록** 탭을 선택하여 각 채널에 기록되는 메세지 범주를 지정하십시오.

문제 해결 추가 정보

as400_joblog 채널 디폴트 심각도 레벨은 Error로 설정됩니다. 이 설정 값은 정보 메세지와 경고 메세지 볼륨을 줄이는 데 사용되며, 볼륨을 줄이지 않을 경우에는 성능이 저하됩니다. 문제가 있지만 작업 기록부가 문제의 요인을 나타내지 않을 경우 심각도 레벨을 변경해야 합니다. 위 프로시듀어를 따라 채널 페이지에 액세스하여 기록 자료를 자세히 볼 수 있도록 as400_joblog 채널의 심각도 레벨을 Warning, Notice 또는 Info로 변경하십시오. 일단 문제가 해결되면, 심각도 레벨을 Error로 재설정하여 작업 기록부의 메세지 수를 줄이십시오.

DNS 디버그 설정

DNS 디버그 기능은 DNS 서버 문제점을 판별하고 정정하는 데 도움이 되는 정보를 제공합니다. 먼저 기록부를 사용하여 문제점을 정정할 것을 권장합니다.

유효한 디버그 레벨은 0-11입니다. DNS 문제점을 진단하기 위해 적절한 디버그 값을 판별하는 데 IBM 서비스 담당자가 도움을 줄 것입니다. 값이 1 이상이면 iSeries 디렉토리 경로 **Integrated File System/Root/QIBM/UserData/OS400/DNS/<serverinstance>**(여기서, ″<server instance>″는 DNS 서버 인스턴스명)에 있는 NAMED.RUN 파일에 디버그 정보를 기록합니다. NAMED.RUN 파일은 디버그 레벨 1 이상으로 설정되어 있으며 DNS 서버가 실행을 계속하는 동안 점점 증가합니다. 수시로 파일을 삭제하여 디스크 공간을 너무 많이 차지하지 않도록 하십시오. **서버 등록 정보 - 채널** 페이지를 사용하여 NAMED.RUN 파일의 버전 번호와 최대 *크기* 기본설정을 지정할 수 있습니다.

DNS 서버 인스턴스의 디버그 값을 변경하려면 다음과 같이 하십시오.

1. **iSeries Navigator**에서 **사용자 iSeries 서버** —> **Network** —> **서버** —> **DNS**를 확장하십시오.
2. 오른쪽 분할 창에서 **사용자 DNS 서버**를 오른쪽 마우스 버튼으로 클릭하고 **구성**을 선택하십시오.
3. **DNS 구성** 창에서 DNS 서버를 오른쪽 마우스 버튼으로 클릭하고 **등록 정보**를 선택하십시오.
4. **서버 등록 정보 - 일반** 페이지에서 서버 시작 디버그 레벨을 지정하십시오.

5. 서버가 작동하고 있으면 서버를 중단했다가 재시작하십시오.
   주: 디버그 레벨에 대한 변경은 서버가 작동하는 중에는 적용되지 않습니다. 여기서 설정한 디버그 레벨 설정은 다음에 서버를 재시작했을 때 사용됩니다. 서버가 작동하는 동안 디버그 레벨을 변경해야 하는 경우 확장 DNS 피처를 참조하십시오.

기타 DNS 정보

DNS 및 BIND 8과 관련하여 참조할 수 있는 정보 소스에는 여러 가지가 있습니다. 다음 리스트는 사용할 수 있는 자원 중 극히 일부만 표시한 것입니다.

- DNS 및 BIND, 제3판. Paul Albitz와 Cricket Liu 공저. 출판사: O'Reilly and Associates, Inc.

  Sebastopol,California,1998. ISBN 번호: 1-56592-512-2. 이것은 DNS에 관해 가장 명료한 설명을 제공하는 소스입니다.
- Internet Software Consortium 웹 사이트

  에는 뉴스, 링크 및 다른 BIND 자원이 들어 있습니다.
- InterNIC

  사이트는 ICANN(Internet Corporation for Assigned Names and Numbers)이 공인한 정의역명 등록 기관 디렉토리를 유지보수합니다.
- DNS Resources Directory

  는 DNS 참조 자료를 제공하며, 토론 그룹을 포함한 다수의 기타 DNS 자원에 링크합니다. 또한 DNS 관련 RFC

  리스트를 제공합니다.

IBM 매뉴얼 및 레드북

- AS/400 TCP/IP Autoconfiguration: DNS and DHCP Support

  이 레드북은 OS/400에 포함된 정의역명 시스템(DNS) 서버와 동적 호스트 구성 프로토콜(DHCP) 서버 지원에 대해 설명합니다. 이 레드북의 정보는 예를 통해 DNS와 DHCP 지원을 설치, 조정, 구성하고 문제점

을 해결할 수 있도록 도와줍니다.

주: 이 레드북은 V5R1에 사용할 수 있는 신규 BIND 8 피처를 포함시켜 갱신된 것이 아닙니다. 그러나 일반적인 DNS 개념을 파악하기 위해서는 훌륭한 참조서입니다.

Printed in U.S.A