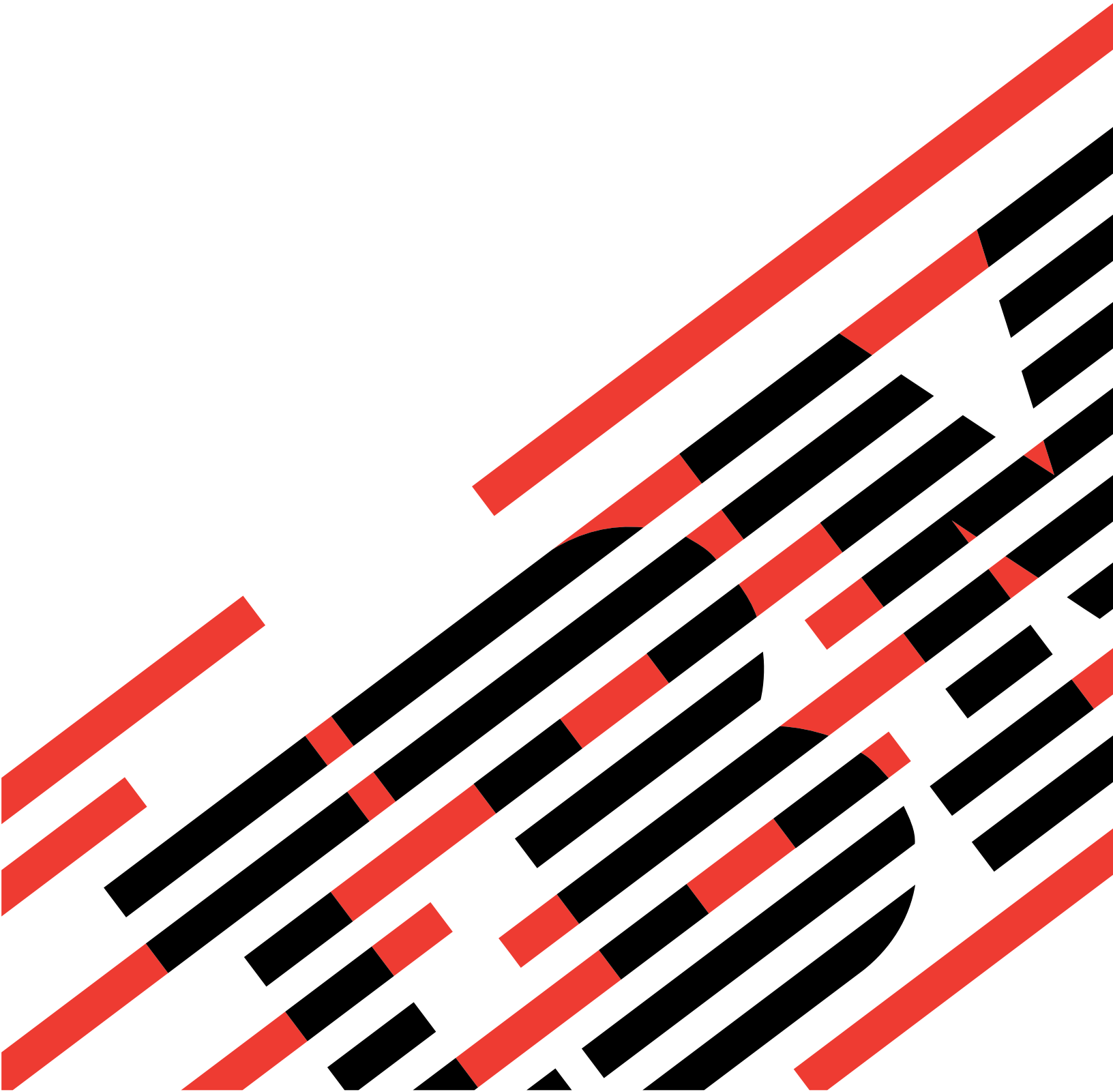
IBM

eserver

iSeries

DNS



IBM

@server

iSeries

DNS

本マニュアルに関するご意見やご感想は、次の URL からお送りください。今後の参考にさせていただきます。

http://www.ibm.com/jp/manuals/main/mail.html

なお、日本 IBM 発行のマニュアルはインターネット経由でもご購入いただけます。詳しくは

http://www.ibm.com/jp/manuals/ の「ご注文について」をご覧ください。

(URL は、変更になる場合があります)

原　典： RZAK–K000–01
iSeries
DNS

発　行： 日本アイ・ビー・エム株式会社

担　当： ナショナル・ランゲージ・サポート

第1刷 2002.8

目次

DNS 1
V5R1 の新機能 2
トピックの印刷 3
DNS 例 3
例 : イントラネット用の単一 DNS サーバー 3
例 : インターネット・アクセスを行う単一 DNS サーバー 5
例 : 同一 iSeries サーバー上に DNS および DHCP 6
例 : ファイアウォールでの分割 DNS 7
DNS の概念 9
DNS について 10
DNS 照会について 11
ご使用の DNS ドメインのセットアップ 12
動的更新 13
BIND 8 機能 14
DNS リソース・レコード 15
メールおよび MX レコード 15
DNS 計画 16
DNS 権限の決定 16
ドメイン構造の決定 16
セキュリティー基準の計画 17
DNS システム要件 18
DNS 構成 19
iSeries ナビゲーターでの DNS のアクセス方法 19
ネーム・サーバーの構成 20
動的更新を受信するための DNS の構成方法 22
DNS ファイルのインポート 22
外部 DNS データ・アクセス 23
DNS 管理 24
NSLookup による DNS 機能の検証 24
セキュリティー・キー管理 25
DNS サーバー統計 25
DNS 構成ファイルの維持管理 26
拡張 DNS 機能 29
DNS のトラブルシューティング 30
DNS サーバー・ロギング 30
DNS デバッグ設定 32
DNS に関するその他の情報 33

DNS

ドメイン・ネーム・システム (DNS) は、ホスト名およびそれに関連するインターネット・プロトコル (IP) アドレスを管理するための分散データベース・システムです。 DNS を使用することは、簡単な名前 (ホストを見付ける場合に、IP アドレス xxx.xxx.xxx.xxx ではなく、“www.jkltoys.com” など) を使用できることを意味します。単一のサーバーの場合、ゾーンの小さなサブセットに対するホスト名と IP アドレスを知っているだけでもかまいませんが、DNS サーバーの場合は、すべてのドメイン・ネームを IP アドレスにマッピングするように協同する必要があります。協同する DNS サーバーは、コンピューターがインターネット全体にわたって通信できるようにするサーバーです。

バージョン 5 リリース 1 (V5R1) では、DNS サービスは BIND (Berkeley Internet Name Domain) バージョン 8 と呼ばれる業界標準の DNS インプリメンテーションに基づいています。以前の OS/400(R) DNS サービスは BIND バージョン 4.9.3 に基づいていました。 OS/400 オプション 33 ポータブル・アプリケーション・ソリューション環境 (PASE) は、新しい BIND 8 ベースの DNS サーバーを使用するために、iSeries(TM) サーバー上にインストールされている必要があります。 PASE がインストールされていない場合、以前のリリースで使用可能となった DNS サーバー (BIND 4.9.3 ベース) と同じものを継続して実行することができます。

注: このトピックでは、BIND 8 に基づく新機能を説明します。PASE を使用せずに BIND 8 ベースの DNS を実行する場合、BIND 4.9.3 ベースの DNS 関連情報について、V4R5 Information Center にある DNS  を参照してください。

- V5R1 の新機能では OS/400 DNS に対する更新を説明します。
- トピックの印刷では、DNS トピックをダウンロードまたは印刷できるようになります。

DNS の理解

このトピックは、iSeries 用 DNS の基本を理解するのに有効です。

DNS 例 は DNS の機能を図解し、説明します。

DNS 概要 では、DNS が機能するのに使用されるオブジェクトとプロセスを説明します。

DNS 計画は、ご使用の DNS 構成の計画作成に有効です。

DNS の使用方法

このトピックは、iSeries 上の DNS を構成および管理する場合に有効です。今回、使用可能になった新機能の利用方法についても説明します。

DNS システム要件

このトピックでは、iSeries 上で DNS を稼動するためのソフトウェア要件を説明します。

DNS 構成

このトピックでは、ネーム・サーバーを構成し、自分以外のドメインで照会に応答するための iSeries ナビゲーターの使用方法を説明します。

DNS 管理

このトピックでは、DNS 機能の検証方法、パフォーマンス・モニター方法、および DNS データとファイルの管理方法について説明します。

DNS のトラブルシューティング
このトピックでは、DNS サーバーに発生した問題を解決するのに有効な、DNS ロギングおよびデバッグ設定について説明します。

Information Center で回答できないご質問がありましたら、DNS に関するその他の情報で、その他のリソースと参照資料を提供しています。

V5R1 の新機能

新ソフトウェア機能

バージョン 5 リリース 1 (V5R1) では、DNS インターフェースが再設計されました。 V5R1 DNS サービスは BIND (Berkeley Internet Name Domain) バージョン 8 と呼ばれる業界標準の DNS インプリメンテーションに基づいています。以前の OS/400 DNS サービスは BIND 4.9.3 に基づいていました。

OS/400 オプション 33 ポータブル・アプリケーション・ソリューション環境 (PASE) は、新しい BIND 8 ベースの DNS サーバーを使用するために、iSeries サーバー上にインストールされている必要があります。詳しくは、DNS システム要件を参照してください。

PASE がインストールされていない場合、BIND 8 の新機能を利用できません。ただし、以前のリリースで使用可能となった DNS サーバー (BIND 4.9.3 ベース) と同じものを継続して実行することができます。

BIND 4.9.3 ベースの DNS 関連情報については、V4R5 Information Center にある DNS を参照してください。

BIND 8 でサポートされる新機能の 1 つに、動的更新があります。ご使用の DNS サーバーをセットアップして、動的リソース・レコード更新を DHCP とその他の許可されたソースから保護できるようになります。 BIND 8 機能トピックでは、BIND 8 がサポートするその他の新機能を説明します。この新機能には以下があります。

- 単一システム上での複数 DNS サーバー
- 条件付き転送
- 動的更新の保護
- 通知
- 増分ゾーン転送 (IXFR)

新しい情報

V5R1 Information Center DNS トピックは更新されて、BIND 8 に基づく新規 DNS 機能をサポートします。 PASE がインストールされていない場合、以前のリリースで使用可能となった DNS サーバー (BIND 4.9.3 ベース) と同じものを継続して実行することができます。 BIND 4.9.3 ベースの DNS 関連情報については、V4R5 Information Center にある DNS を参照してください。

DNS シナリオでは、サンプルを示して、基本的な DNS 概念を紹介しています。ご使用の iSeries 用の DNS を、計画および構成する場合、このシナリオを参照すると便利です。トラブルシューティング情報は、ご使用のサーバー構成をデバッグするのに入手すると有効です。

トピックの印刷

PDF 版をダウンロードし、表示するには、「DNS」(約 243 KB、40 ページ) を選択してください。

表示用または印刷用の PDF ファイルをワークステーションに保存するには、次のようにします。

1. ブラウザーで PDF を開く (上記のリンクをクリックする)。
2. ブラウザーのメニューから「**ファイル**」をクリックする。
3. 「**名前を付けて保存**」をクリックする。
4. PDF を保存したいディレクトリーに進む。
5. 「**保存**」をクリックする。

PDF ファイルを表示したり印刷したりするには、Adobe Acrobat Reader が必要です。Adobe Web サイト (www.adobe.com/products/acrobat/readstep.html) からダウンロードできます。

DNS 例

DNS は、ホスト名およびその関連 IP アドレスを管理するための分散データベース・システムです。以下の例は、DNS の機能およびご使用のネットワーク上でそれを使用可能にする方法を説明するのに、有効です。この例には、そのセットアップおよび使用される理由が説明されています。各例には、その図を理解するのに有効と思われる関連概念へのリンクがあります。

例 : イントラネット用の単一 DNS サーバー
内部使用のための DNS サーバーを持った単純なサブネットを図示します。

例 : インターネット・アクセスを伴う単一 DNS サーバー
インターネットに直接接続された DNS サーバーを持った単純なサブネットを図示します。

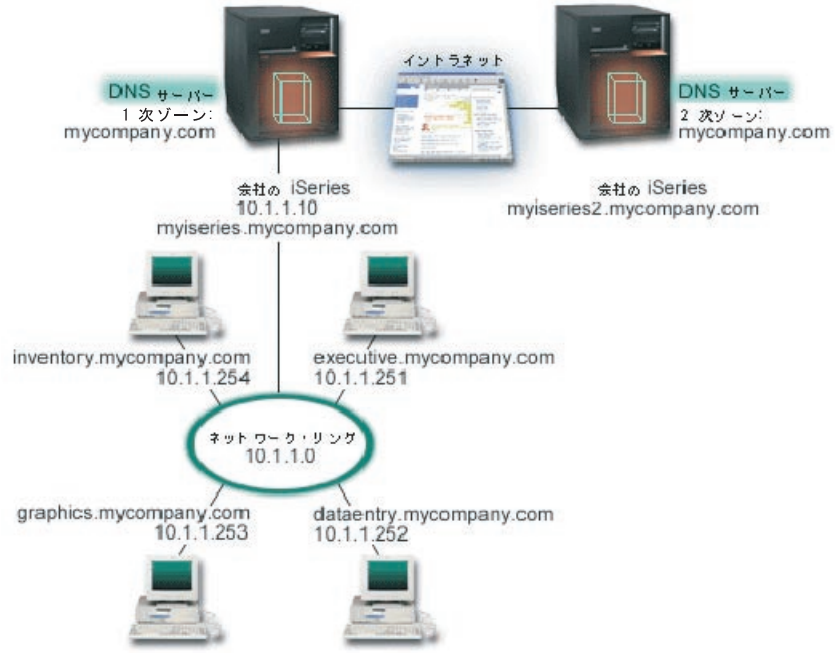
例 : 同一 iSeries サーバー上に DNS および DHCP
同一サーバー上に DNS および DHCP を図示します。この構成は、DHCP が IP アドレスをホストに割り当てた場合に、DNS ゾーン・データを動的に更新するのに使用できます。ご使用の DHCP サーバーが別の iSeries 上にある場合、追加の DHCP 構成要件に関しては、例 : DNS と DHCP が異なる iSeries サーバー上にある場合を参照してください。

例 : ファイアウォールでの分割 DNS
インターネットから内部データを保護するためのファイアウォールを通じて稼働する DNS を図示します。一方で、内部ユーザーはインターネット上のデータをアクセスできます。

例 : イントラネット用の単一 DNS サーバー

次の図は、内部ネットワーク用の iSeries 上で稼動する DNS を図示しています。この単一 DNS インスタンスは、全インターフェースの IP アドレス上で照会を listen するようにセットアップされています。このサーバーは「mycompany.com」ゾーン用の 1 次ネーム・サーバーです。

図 1. イントラネット用の単一 DNS サーバー



ゾーン内の各ホストには、IP アドレスとドメイン・ネームが付いています。管理者は、リソース・レコードを作成することにより、手動で DNS ゾーンにあるホストを定義する必要があります。アドレス・マッピング (A) レコードは、マシンの名前をその関連 IP アドレスにマップします。これにより、ネットワーク上の他のホストが DNS サーバーに照会して、特定ホスト名に割り当て済みの IP アドレスを見付けることができるようになります。逆検索ポインター (PTR) レコードは、マシンの IP アドレスをその関連ホスト名にマップします。これにより、ネットワーク上の他のホストが DNS サーバーに照会して、IP アドレスに関連したホスト名を見付けることができるようになります。

A および PTR レコードに加えて、DNS は多くの必要な他リソース・レコードをサポートします。これは、ご使用のイントラネット上で稼動する TCP/IP ベースの他アプリケーションが何であるかにより異なります。たとえば、内部的な E-mail システムを実行している場合、メール・エクスチェンジャー (MX) レコードを追加する必要があります。それによって SMTP は、どのシステムがメール・サーバーを実行しているかを見付けるために DNS に照会することができます。

この小規模のネットワークが、より大規模なイントラネットの一部の場合、内部的なルート・サーバーを定義する必要があります。

2 次サーバー

2 次サーバーはゾーン・データをオーソリタティブ・サーバーからロードします。 2 次サーバーは、オーソリタティブ・サーバーからゾーンを伝送されてゾーン・データを入手します。 2 次ネーム・サーバーが始動すると、このサーバーは指定ドメインあての全データを 1 次サーバーから要求します。 2 次ネーム・サーバーは、更新済みデータを 1 次サーバーに要求します。この理由は、そのサーバーが 1 次ネーム・サーバーから通知を受信するか (NOTIFY (14を参照してください。) 機能が使用されている場合)、1 次ネーム・サーバーに照会した結果、データが変更されていることが判明したか、のいずれかです。
上記の図では、サーバー「myiseries」はイントラネットの一部です。もう 1 つの iSeries サーバー「myiseries2」は、mycompany.com zone 用の 2 次サーバーとして機能するように構成されています。2 次サーバーを使用して、サーバーにかかる要求を分散することができます。また、1 次サーバー障害時のバックアップとしても使用することができます。各ゾーンごとに最低 1 つの 2 次サーバーを持つことが、実質的に有効です。

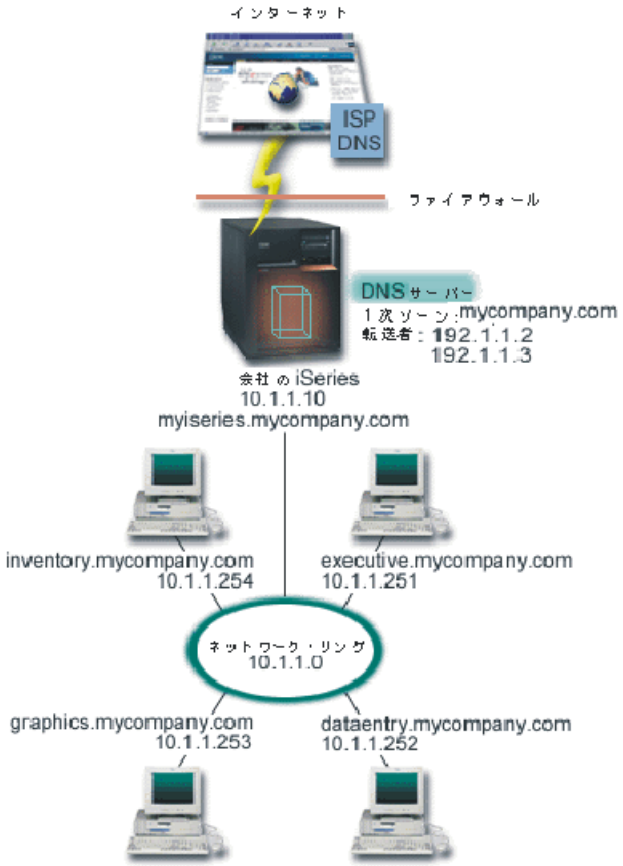
この例で説明されたオブジェクトについての詳細は、以下のトピックを参照してください。

- DNS についてでは、DNS が何か、およびその機能を説明しています。 DNS サーバー上で定義可能な種々のゾーン・タイプも説明されています。
- DNS リソース・レコードには、DNS によるリソース・レコードの使用方法が説明されています。

例 : インターネット・アクセスを行う単一 DNS サーバー

次の図では、イントラネット用の単一 DNS サーバーの例と同じネットワーク例を図示していますが、ここでは、インターネットへの接続を追加しました。この例では、この会社はインターネットにアクセスすることができますが、インターネットからこの会社のネットワークへのアクセスは、ファイヤーウォールによりブロックされるように構成されています。

図 1. インターネット・アクセスを行う単一 DNS サーバー



IP アドレスを解決するには、以下の 1 つを少なくとも実施する必要があります。

インターネット・ルート・サーバーの定義
デフォルトのインターネット・ルート・サーバーを自動的にロードできますが、そのリストを更新する必要がある場合があります。これらのサーバーは、自分自身のゾーン外のアドレスを解決するのに有効です。 現行のインターネット・ルート・サーバーを入手する方法は、外部 DNS データのアクセス方法を参照してください。

転送を使用可能にする
外部の DNS サーバー (インターネット・サービス提供者 (ISP) が実行している DNS サーバーなど)

に対して mycompany.com のゾーン外のアドレス照会を渡す転送をセットアップすることができます。転送方式およびルート・サーバー方式の両方による検索を使用可能にしたい場合、**forward** オプションを **first** に設定する必要があります。このサーバーは最初に転送方式を行ってから、そこでアドレス解決ができなかった場合にルート・サーバーに照会します。

以下の構成変更も必要となる場合があります。

無制限の IP アドレス割り当て
上記の例では、10.x.x.x のアドレスが示されています。しかし、これらは制約されたアドレスであり、イントラネット外では使用できません。このアドレスは、例示目的用に以下に示されていますが、自分自身の IP アドレスは ISP または他のネットワーキング要因によって決定されます。

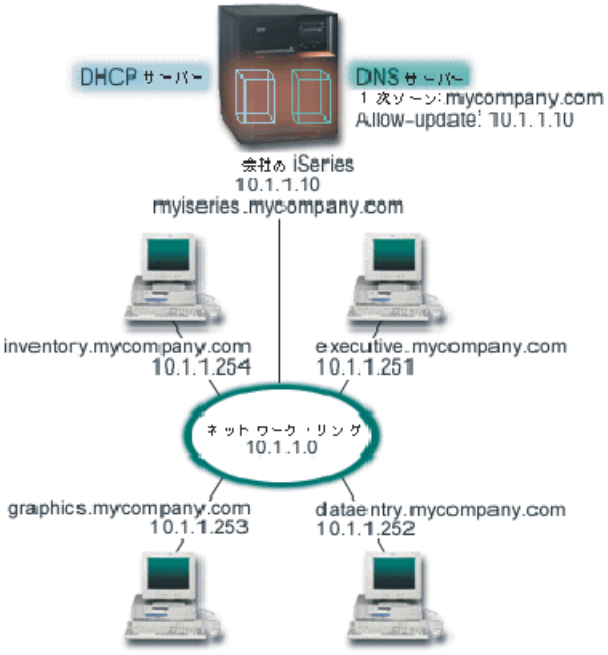
自分のドメイン・ネームの登録
インターネットからアクセスできるようにする場合で、まだドメイン・ネームが登録されていない場合、ドメイン・ネームの登録を行う必要があります。

ファイアウォールの確立
ご使用の DNS がインターネットに直接接続されるようにすることはお勧めできません。ファイアウォールを構成するか、他の予防措置を講じて、ご使用の iSeries を保護してください。詳しくは、Information Center にある IBM SecureWay: iSeries およびインターネットを参照してください。

例 : 同一 iSeries サーバー上に DNS および DHCP

次の図では、4 つのクライアントに対して DNS と DHCP サーバーとして機能する 1 つの iSeries サーバーを持った、小規模のサブネット・ネットワークが図示されています。この稼動環境で、在庫、データ入力、経営者の各クライアントがグラフィックス・ファイル・サーバーでグラフィックスの資料を作成すると仮定します。各クライアントは、そのホスト名に対するネットワーク・ドライブによりグラフィックス・ファイル・サーバーに接続します。

図 1. 同一 iSeries サーバー上に DNS および DHCP



以前のバージョンの DHCP と DNS はお互いに独立していました。 DHCP がクライアントに新しい IP アドレスを割り当てた場合、DNS レコードを管理者が手動で更新する必要がありました。この例では、グラフィックス・ファイル・サーバーの IP アドレスが DHCP により変更された場合、そこにアクセスするクライアントはネットワーク・ドライブをそのホスト名にマップできなくなります。理由は、DNS レコードが以前のファイル・サーバーの IP アドレスを持っているからです。

BIND 8 に基づく V5R1 DNS サーバーにより、ご使用の DNS ゾーンを構成して、DHCP による一時的なアドレス変更に関連して、DNS レコードに対する動的更新を受け入れるようにします。たとえば、グラフィックス・ファイル・サーバーがそのリースを更改して、新たに IP アドレス 10.1.1.250 を DHCP が割り当てた場合、関連する DNS レコードは動的に更新されます。これによりその他のクライアントが、グラフィックス・ファイル・サーバー用の DNS サーバーをそのホスト名で、中断せずに照会できるようになります。

DNS ゾーンを構成して動的更新を受け入れるには、以下の作業を完了してください。

動的ゾーンの識別化
サーバー稼動中は手動で動的ゾーンを更新することができません。それを行うと、入ってくる動的更新に悪影響を及ぼします。手動による更新ができるのは、サーバーの停止後です。ただし、サーバー停止中に送信された動的更新はすべて失われます。この理由により、手動による更新の必要性を最小限にするために、分離された動的ゾーンを構成することができます。動的更新機能を使用するためのゾーン構成方法の詳細は、ドメイン構造の決定を参照してください。

更新許可オプションの構成
更新許可オプションで構成されたすべてのゾーンは、動的ゾーンと考えられます。更新許可オプションはゾーン単位ベースで設定されます。動的更新を受け入れるには、更新許可オプションがこのゾーンで使用可能になっている必要があります。この例では、mycompany.com ゾーンは更新許可データを持っていますが、サーバー上に定義された他のゾーンは、静的または動的として構成できます。

動的更新を送信する DHCP 構成
ご使用の DHCP サーバーによる、分散された IP アドレス用 DNS レコードの更新を許可する必要があります。動的更新を送信するように DHCP サーバーを構成する方法の詳細は、動的更新を送信するための DHCP の構成を参照してください。

2 次サーバーの更新プリファレンスの構成
2 次サーバーを最新状態に保つために、NOTIFY (14を参照してください。) を使用するように DNS を構成することができます。これは、ゾーン・データ変更時に mycompany.com ゾーン用の 2 次サーバーにメッセージを送信するためです。増分ゾーン転送 (IXFR) (14を参照してください。) も構成する必要があります。これにより、IXFR 対応の 2 次サーバーが、ゾーン全体ではなく、更新されたゾーン・データのみをトラッキングおよびロードできるようになります。

別のサーバー上で DNS と DHCP を稼動させた場合、DHCP サーバーに対していくつかの追加構成要件があります。詳しくは、例 : 別 iSeries サーバー上の DNS および DHCP を参照してください。

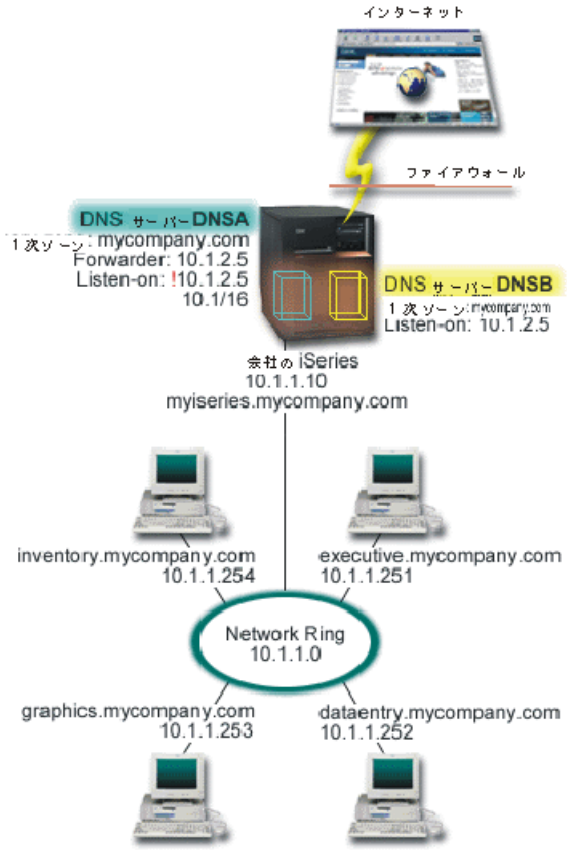
例 : ファイアウォールでの分割 DNS

次の図には、セキュリティー用のファイアウォールを使用した単純なサブネット・ネットワークが図示されてます。 BIND 8 に基づく V5R1 DNS により、単一 iSeries 上で複数 DNS サーバーをセットアップできるようになります。この企業には、予約済みの IP スペースを持った内部ネットワーク、および外部に対し使用可能なネットワークの外部セクションがあると仮定します。

この企業では、その内部クライアントが外部のホスト名を解決できるようにして、外部の人たちとメール交換できるようにしたいと考えています。この企業はまた、その内部リゾルバーが、内部ネットワーク範囲外では利用不能な内部用だけのゾーンにアクセスできるようにしたいとも考えています。しかし、いかなる外側リゾルバーも内部ネットワークにはアクセスできないようにしたいと考えています。

これを行うには、この企業では 2 つの DNS サーバー・インスタンスを同一 iSeries 上にセットアップします。 1 つはイントラネット用、もう 1 つはパブリック・ドメイン用です。これを分割 DNS と呼びます。

図 1. ファイアウォールでの分割 DNS



外部サーバーの DNSB は、1 次ゾーン mycompany.com で構成されています。このゾーンには、パブリック・ドメインの一部として意図されたリソース・レコードが含まれています。内部サーバーの DNSA は、1 次ゾーン mycompany.com で構成されていますが、DNSA 上に構成されたゾーン・データにはイントラネット・リソース・レコードが含まれています。 forwarders オプションには 10.1.2.5 と定義されています。このオプションにより、DNSA が 自分で解決できないアドレス照会を DNSB に強制的に転送します。

ファイアウォールのセキュリティーまたは他のセキュリティーへの脅威を心配している場合、内部データを保護するのに有効な listen-on オプションを使用する選択肢があります。これを行うためには、内部ホストから内部 mycompany.com ゾーンへ照会できるように、内部サーバーを構成することができます。これらすべてが正しく機能するには、内部クライアントは DNSA サーバーのみに照会するように構成する必要があります。分割 DNS をセットアップするには、以下の構成設定を考慮する必要があります。

Listen-on

前述の例では、iSeries 上には 1 つの DNS サーバーしかありませんでした。このサーバーはすべてのインターフェース IP アドレスを listen-on するように設定されていました。 1 つの iSeries 上に複数の DNS サーバーがある時はいつも、各サーバーが listen-on するインターフェース IP アドレスを定義する必要があります。 2 つの DNS サーバーは、同一アドレスを listen-on することはできません。この場合は、ファイアウォールから入ってくるすべての照会は、10.1.2.5 上に送信されると仮定します。これらの照会は外部サーバーへ送信される必要があります。このため、DNSB は 10.1.2.5 で listen するように構成されます。内部サーバーの DNSA は、10.1.2.5 *以外* の 10.1.x.x 1 IP アドレスのいずれからでも、照会を受け入れるように構成されています。このアドレスを効率的に除外するには、アドレス・マッチ・リスト (AML) は、アドレス接頭部を組み込む前に、除外対象アドレスをリストしておく必要があります。

アドレス・マッチ・リスト (AML) の順序

指定されたアドレスと一致する AML 中の最初の要素が使用されます。たとえば、10.1.x.x ネットワーク上の 10.1.2.5 以外の全アドレスを許可するには、ACL 要素は (!10.1.2.5; 10.1/16) の順序になっている必要があります。この場合、アドレス 10.1.2.5 は最初の要素と比較されて、即時に除外されます。

この要素が (10.1/16; !10.1.2.5) のように逆になっていると、IP アドレス 10.1.2.5 はアクセスを許可されてしまいます。理由は、サーバーはそのアドレスを最初の要素と比較し、それが一致すると残りのルールをチェックせずに許可してしまいます。

DNS の概念

V5R1 DNS は、BIND 8 に基づく新機能を提供します。以下のリンクには、DNS の機能および使用可能な新機能の概要が説明されています。

基本 DNS 機能

DNS について

DNS の機能概要と、定義可能なゾーン・タイプの説明が提供されています。

DNS 照会について

DNS がクライアントに代わってアドレスを解決する方法が説明されています。

ご使用の DNS ドメインのセットアップ

ドメイン登録の概要と、それに伴い、自分自身のドメイン・スペース・セットアップ用の他の参照サイトへのリンクが提供されています。

新 DNS 機能

動的更新

V5R1 DNS (BIND 8 ベース) は動的更新をサポートします。これにより、DHCP などの外部ソースが DNS サーバーに更新を送信できるようになります。

BIND 8 機能

動的更新以外に、BIND 8 はご使用の DNS サーバーの性能を向上するいくつかの新機能を提供しています。

リソース・レコード参照

DNS リソース・レコード
リソース・レコードは、ドメイン・ネームと IP アドレスに関するデータを格納するのに使用されます。このトピックには、V5R1 でサポートされるリソース・レコードの検索可能リストが含まれています。

メールおよび MX リソース・レコード
DNS は、このレコードの使用により、拡張メール・ルーティングをサポートします。

非常に詳細に DNS を説明している多くの外部ソースがあります。その他の参照先として、DNS に関するその他の情報を参照してください。

DNS について

ドメイン・ネーム・システム (DNS) は、ホスト名およびそれに関連するインターネット・プロトコル (IP) アドレスを管理するための分散データベース・システムです。 DNS を使用することは、簡単な名前 (ホストを見付ける場合に、IP アドレス xxx.xxx.xxx.xxx ではなく、“www.jkltoys.com” など) を使用できることを意味します。単一のサーバーの場合、ゾーンの小さなサブセットに対するホスト名と IP アドレスを知っているだけでもかまいませんが、DNS サーバーの場合は、すべてのドメイン・ネームを IP アドレスにマッピングするように協同する必要があります。協同する DNS サーバーは、コンピューターがインターネットを通じて通信できるようにするサーバーです。

DNS データは、ドメイン階層に分解されます。サーバーは、単一のサブドメインなどのデータのほんの一部分を知っているだけです。そのサーバーが直接管理する必要があるドメイン部分はゾーンと呼ばれます。1 つのゾーンに対する完全なホスト情報とデータを持っている DNS サーバーは、そのゾーンに対して許可されていると言えます。オーソリタティブ・サーバーは、そのゾーン内のホストに関する照会に、独自のリソース・レコードを使用して応答することができます。その照会プロセスは、複数の要素により決まります。DNS 照会についてでは、クライアントが照会に対応するのに使用できる経路を説明します。

ゾーンについて

DNS データは、ゾーンとよばれる管理可能なデータのセットに分割されます。ゾーンには、1 つの DNS ドメインの一部または複数部分に関する名前および IP アドレスが含まれています。1 つのゾーンに対する情報すべてを含んだサーバーは、そのドメインに対するオーソリタティブ・サーバーです。場合によっては、特定のサブドメインに対する DNS 照会の応答権限を別の DNS サーバーに代行させることは意味のあることです。この場合、そのドメインに対する DNS サーバーはそのサブドメイン照会が該当のサーバーを参照するように構成することができます。

障害時のバックアップと冗長性を考慮して、ゾーン・データはオーソリタティブ DNS サーバー以外のサーバー上に格納するのが普通です。この別サーバーは 2 次サーバーと呼ばれ、オーソリタティブ・サーバーからゾーン・データをロードします。2 次サーバーを構成することにより、サーバーにかかる要求をバランスできるようになるとともに、1 次サーバー・ダウン時のバックアップを提供できるようにもなります。2 次サーバーは、オーソリタティブ・サーバーからゾーンの転送を行うことによってゾーン・データを入手します。2 次サーバーの初期化時に、1 次サーバーからゾーン・データの完全コピーをロードします。2 次サーバーもまた、ゾーン・データ変更時にそのドメインに対して、1 次サーバーかまたは他の 2 次サーバーからゾーン・データを再ロードします。

DNS ゾーン・タイプ

iSeries DNS を使用して、DNS データの管理に有効な、以下に示すいくつかのゾーン・タイプを定義できます。

1 次ゾーン
ホスト上のファイルから直接ゾーン・データをロードします。1 次ゾーンにはサブゾーンまたは子ゾーンが

含まれる場合があります。1 次ゾーンにはリソース・レコード (ホスト、別名 (CNAME)、アドレス (A)、または逆マッピング・ポインター (PTR) レコードなど) が含まれる場合もあります。
注 : 場合によっては、1 次ゾーンは、他の BIND 資料で「マスター・ゾーン」と呼ばれます。

サブゾーン
サブゾーンは 1 次ゾーン内のゾーンを定義します。サブゾーンにより管理可能な断片にゾーン・データを編成できるようにします。

子ゾーン
子ゾーンはサブゾーンを定義し、サブゾーン・データに対する責任を 1 つまたは複数のネーム・サーバーに代行させます。

別名 (CNAME)
別名は、1 次ドメイン・ネームに対する代替名を定義します。

ホスト
ホスト・オブジェクトは、A と PTR レコードをホストにマッピングします。追加のリソース・レコードがホストに関連付けられる場合があります。

2 次ゾーン
ゾーン・データをゾーンの 1 次サーバーまたは別の 2 次サーバーからロードします。 2 次サーバーは、そのゾーン・データがセカンダリーとなるゾーンの完全コピーを管理します。
注 : 場合によっては、2 次ゾーンは、他の BIND 資料で「スレーブ・ゾーン」と呼ばれます。

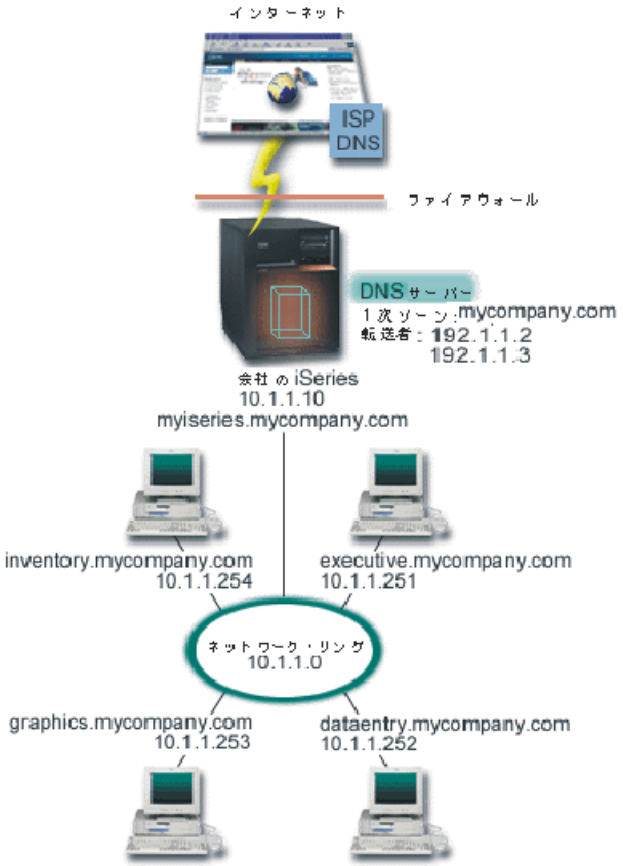
スタブ・ゾーン
スタブ・ゾーンは、2 次ゾーンに似ていますが、そのゾーンに対するネーム・サーバー (NS) レコードだけを転送します。

フォワード・ゾーン
フォワード・ゾーンは、その特定ゾーンあてのすべての照会を他のサーバーに転送します。

DNS 照会について

クライアントは DNS サーバーを使用して、そのサーバーから情報を見付けます。 その要求はクライアントから直接入ってくることも、またはクライアント上で実行中のアプリケーションから入ってくることもあります。クライアントは照会メッセージを DNS サーバーに送信します。そのメッセージには、完全修飾のドメイン・ネーム (FQDN)、照会タイプ (クライアントが要求する特定リソース・レコードなど)、およびドメイン・ネームのクラス (これは通常、インターネット (IN) クラス) が含まれます。以下の図には、インターネット・アクセスを行う単一 DNS サーバーのサンプル・ネットワークが図示されています。

図 1. インターネット・アクセスを行う単一 DNS サーバー



ホスト *dataentry* は 「graphics.mycompany.com」に関して DNS サーバーに照会すると仮定します。DNS サーバーは自分自身が持っているゾーン・データを使用して、IP アドレス 10.1.1.253 について応答します。

ここで、*dataentry* は IP アドレス「www.jkl.com.」を要求すると仮定します。このホストは、この DNS サーバーのゾーン・データ内にはありません。たどれる経路には、再帰または反復の 2 つがあります。DNS サーバーは、再帰を使用するように設定されている場合、このサーバーは、要求側のクライアントに代わって名前を完全に解決するために他の DNS サーバーに照会または連絡してからクライアントに回答を戻します。DNS サーバーが別 DNS サーバーに照会する場合、要求側のサーバーはその回答を自分のキャッシュに入れておき、次回同じ照会を受けたときに使用します。クライアントは、自分自身で名前を解決する代わりに、他の DNS サーバーに連絡してみることができます。反復と呼ばれるこのプロセスでは、サーバーからの照会の応答に基づいて、クライアントは別個の追加の照会を使用します。

ご使用の DNS ドメインのセットアップ

DNS により、イントラネットまたは内部ネットワーク上の名前とアドレスを提供できるようになります。DNS により、インターネット経由で他の世界の名前とアドレスも提供できるようになります。インターネット上のドメインをセットアップしたい場合、ドメイン・ネームを登録するように要求されます。

イントラネットを設定している場合、内部使用のためにドメイン・ネームを登録する必要はありません。イントラネット名を登録するかどうかは、内部的な使用とは関係なく、インターネット上でその名前を誰にも使用できないようにしたいかどうかに依存します。内部的に使用予定の名前を登録することは、後でそのドメイン・ネームを外部的に使用したい場合に決して矛盾を起こさないことを保証します。

ドメイン登録は、許可されたドメイン・ネーム登録機関に直接連絡して行うか、または一部のインターネット・サービス提供者 (ISP) により行います。一部の ISPでは、ドメイン・ネーム登録要求を代行して依頼するサービスを提供しています。 Internet Network Information Center (InterNIC)  は、すべてのドメイン・ネーム登録機関のディレクトリーを管理しています。これは、Internet Corporation for Assigned Names and Numbers (ICANN) によって認可されています。

ホストに対して DNS ドメインを登録および準備するための情報提供している、多くのソースがあります。詳細は、DNS に関するその他の情報を参照してください。

動的更新

Dynamic Host Configuration Protocol (DHCP) は、中央サーバーを使用してネットワーク全体の IP アドレスおよび他の構成の詳細を管理する TCP/IP 標準です。 DHCP サーバーはクライアントからの要求に応答し、クライアントにプロパティーを動的に割り当てます。 DHCP により、中央でネットワーク・ホスト構成パラメーターを定義し、ホストの構成を自動化できます。 DHCP を使用して、使用可能な IP アドレス数よりも多くのクライアントを持ったネットワーク用に、一時的 IP アドレスをクライアントに割り当てることがあります。

過去には、すべての DNS データは静的なデータベースに格納されていました。すべての DNS リソース・レコードの作成と保守を管理者が行わなければなりませんでした。現在では、BIND 8 で稼動する DNS サーバーはゾーン・データを動的に更新する他ソースからの要求を受け入れるように構成されています。

ご使用の DHCP サーバーを構成して、ホストに新しいアドレスが割り当てられるたびに、DNS サーバーに更新要求を送信することができます。この自動化されたプロセスにより、TCP/IP ネットワークの急速な増大または変更に関する DNS サーバーの管理作業を軽減します。ホスト・ロケーションが頻繁に変更されるネットワークでも同様です。 DHCP を使用しているクライアントが IP アドレスを受信すると、そのアドレスは即時に DNS サーバーに送信されます。この方式を使用して、たとえ IP アドレスがいつ変更されようと、DNS は正確に照会に応答し続けることができます。

DHCP を構成して、アドレスのマッピング (A) レコード、逆検索ポインター (A) レコード、またはその両方を、クライアントに代わって更新できます。A レコードはマシンのホスト名をその IP アドレスにマッピングします。PTR レコードは、マシンの IP アドレスをそのホスト名にマッピングします。クライアントのアドレスが変更された場合、DHCP は自動的に更新を DNS サーバーに送信します。それにより、ネットワーク中のホストがその新 IP アドレスで DNS 照会することにより、クライアントを見付けられるようにします。動的に更新される各レコードごとに、関連テキスト (TXT) レコードが書き込まれて、そのレコードが DHCP により作成されたことを明確にします。
注： DHCP が PTR レコードのみ更新するように設定されていると、クライアントからの更新を可能にするように DNS を構成する必要があります。それにより、各クライアントがその A レコードを更新できます。すべての DHCP クライアントが、自分自身の A レコードの更新要求を行うことをサポートするとは限りません。この方式を選択する前に、ご使用のクライアント・プラットフォームの資料を調べてください。

更新を送信可能な、許可されたソースのリストを作成することにより、動的ゾーンは保護されます。個々の IP アドレス、全サブネット、共用の機密鍵 (トランザクション・シグニチャーまたは TSIG と呼ばれる) を使用してサインされたパケット、またはこれらの方式の組み合わせを使用して許可されたソースを定義できます。DNS は、送られてくる要求パケットが許可されたソースから来ていることをリソース・レコードの更新前に検証します。

動的更新は、単一の iSeries サーバー上の DNS と DHCP 間、異なる iSeries サーバー間、または iSeries と動的更新可能な他サーバー間で行うことができます。 iSeries に合わせた動的更新の構成方法について詳しくは、以下のトピックを参照してください。

- 動的更新を受信するための DNS の構成方法
- 動的更新を受信するための DHCP 構成方法
- 動的更新 API QTOBUPT は、動的更新を DNS に送信するサーバー上に必要です。 OS/400 オプション 31 の DNS では自動的にインストールされます。

BIND 8 機能

DNS は BIND 8 を使用して、V5R1 として再設計されました。PASE がインストールされていない場合、以前にリリースされた OS/400 DNS サーバー (BIND 4.9.3 ベース) を継続して構成および実行することができます。 DNS システム要件には、BIND 8 ベースの DNS を iSeries 上で実行するには何が必要かを説明しています。新 DNS の使用により、以下の機能を利用できるようになります。

単一 iSeries 上での複数 DNS サーバーの稼動

以前のリリースでは、唯一の DNS サーバーが構成可能でした。今回、複数 DNS サーバーまたはインスタンスを構成することができます。これによって、サーバー間に論理的な仕切りをセットアップできるようになります。複数インスタンスを作成する場合、各インスタンスごとに明示的に listen-on インターフェース IP アドレスを定義する必要があります。 2 つの DNS インスタンスは同一インターフェースを listen-on できません。

複数サーバーの実用的なアプリケーションは、分割 DNS です。分割 DNS では、1 つのサーバーが内部ネットワークを管理し、2 番目のサーバーが外部からの照会に使用されます。分割 DNS についての詳細は、ファイアウォールでの分割 DNS の例を参照してください。

条件付き転送

条件付き転送により、転送プリファレンスを細かくチューニングするように DNS サーバーを構成できます。サーバーに回答が分からない、すべての照会を転送するようにサーバーを設定できます。グローバル・レベルでの転送を設定できますが、通常の反復による解決を強制したいドメインに対して例外を追加することもできます。または、グローバル・レベルで通常の反復による解決を設定してから、特定のドメイン内で転送を強制することもできます。

動的更新の保護

DHCP および他の許可されたソースは、動的リソース・レコード更新をトランザクション・シグニチャー (TSIG) およびソース IP アドレス許可を使用して送信できます。これにより、許可されたソースだけを更新に使用することが保証されると同時に、手動によるゾーン・データ更新作業が減少します。

動的更新の詳細は、動的更新を参照してください。外部ソースからの更新許可についての詳細は、セキュリティー基準の計画を参照してください。

NOTIFY

NOTIFY がオンになっていると、1 次サーバー上でゾーン・データが更新される時はいつも DNS NOTIFY 通知機能がアクティブになります。1 次サーバーは、管理下の全 2 次サーバーあてにデータが変更された旨のメッセージを送信します。次いで、2 次サーバーは更新済みゾーン・データに対するゾーン転送要求で応答します。これにより、バックアップ・ゾーン・データを同時に保持することができ、2 次サーバーのサポートを向上します。

ゾーン転送 (IXFR および AXFR)

以前では、2 次サーバーがゾーン・データの再ロードを必要とする時はいつも、2 次サーバーは完全なデー

タ・セット自体をすべてのゾーン転送 (AXFR) にロードする必要がありました。BIND 8 では、新ゾーン転送方式をサポートします。それが増分ゾーン転送 (IXFR) です。IXFR は、他サーバーがゾーンを丸ごと転送する代わりに、変分データのみを転送できる方式です。

この方式が 1 次サーバーで使用可能になると、データ変更には、変更がある旨のフラグが割り当てられます。2 次サーバーがゾーン更新を IXFR 方式で要求した場合、1 次サーバーは新しいデータのみを送信します。IXFR 方式が特に有効なのは、ゾーンが動的に更新され、それによる細かいデータ送信のトラフィック負荷を減少させたい場合です。
注： この機能を使用するには、1 次サーバーと 2 次サーバーの両方で IXFR 使用可能となっている必要があります。

DNS リソース・レコード

DNS ゾーン・データベースはリソース・レコードの集まりで構成されています。各リソース・レコードには、特定オブジェクトに関する情報が指定されています。たとえば、アドレス・マッピング (A) レコードは、ホスト名を IP アドレスにマップし、逆検索ポインター (PTR) レコードは、IP アドレスをホスト名にマップします。 サーバーはこれらのレコードを使用して、そのゾーン内のホストあてに照会の応答を行います。詳しくは、以下の表を使用して DNS リソース・レコードを表示してください。

<LABEL for=″table″>表からレコードを選択するか、または以下の 1 語検索を入力します。 <LABEL>

レコードを選択すれば、その説明を表示できます。

メールおよび MX レコード

メールおよび MX レコードは、シンプル・メール転送プロトコル (SMTP) などのメール・ルーティング・プログラムにより使用されます。 iSeries DNS でサポートされるメール・レコード・タイプに関する詳細は、DNS リソース・レコードにある参照テーブルを参照してください。

DNS には、メール・エクスチェンジャー情報を使用して、電子メールを送信するための情報が含まれています。ネットワークが DNS を使用している場合は、SMTP (シンプル・メール転送プロトコル) アプリケーションは単に、TEST.IBM.COM への TCP 接続をオープンして、ホストの TEST.IBM.COM あてのアドレスにメールを配信するわけではありません。 SMTP はまず最初に、DNS サーバーに照会して、メッセージを配信するのに使用できるホスト・サーバーを見付けます。

特定アドレスへのメール配信

DNS サーバーはメール・エクスチェンジャー (MX) レコードと呼ばれるリソース・レコードを使用します。 MX レコードは、ドメインまたはホスト名をプリファレンス値とホスト名にマッピングします。 MX レコードは、通常、1 つのホストが別ホストあてメールを処理するのに使用されるよう、指定するのに使用されます。このレコードはまた、最初のホストにメールが届かなかった場合、別ホストにメールを配信するよう指定するのにも使用されます。言い換えれば、このレコードにより、あるホストあてのメールが別ホストあてに配信できるようになります。

複数 MX リソース・レコードは同一ドメインまたは同一ホスト名に対して存在する場合があります。複数 MX リソース・レコードが同一ドメインまたは同一ホスト名に対して存在している場合、各レコードのプリファレンス (または優先) 値が配信を試行する順序を決定します。最も低いプリファレンス値は、最優先レコードに関連し、最初にそのレコードが試行されます。最優先ホストにメールが届かない場合、メール送信アプリケーションは、次の優先 MX ホストにコンタクトしようとします。ドメイン管理者か、または MX レコード作成者がプリファレンス値を設定します。

DNS サーバーは、その名前が DNS サーバーで許可されているが、それに MX レコードが割り当てられていない場合、MX リソース・レコードの空リストを応答します。この状態が発生すると、メール送信アプリケーションは宛先ホストと直接接続を確立しようとする場合があります。**注 :** ドメイン用の MX レコードで、ワイルド・カード (例 : *.mycompany.com) を使用することはお勧めできません。

例 : ホスト用の MX レコード
以下の例では、プリファレンス指定により、fsc5.test.ibm.com あてのメールをそのホスト自身に配信する必要があります。そのホストにメールが届かなかった場合、システムはメールを psfred.test.ibm.com または mvs.test.ibm.com (psfred.test.ibm.com にも届かなかった場合) に配信します。この例は、MX レコードがどのように指定されるかを示しています。

```
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 計画

DNS は種々のソリューションを提供します。 DNS を構成する前に、ご使用のネットワーク内でどのように DNS を機能させるかを計画しておくことが重要です。ネットワーク構造、パフォーマンス、およびセキュリティーなどのサブジェクトを DNS をインプリメントする前に評価しておく必要があります。 DNS のニーズに対して以下のトピックを検討してください。

DNS 権限の決定
DNS 管理者に対して特別な許可要件があります。許可が意味するセキュリティーについても検討する必要があります。このトピックでは、その要件を説明します。

ドメイン構造の決定
初めてドメインをセットアップする場合、ゾーン作成前にその要求と保守に対する計画が必要です。

セキュリティー基準の計画
DNS はセキュリティー・オプションを提供して、ご使用のサーバーへの外部からのアクセスを制限します。このトピックでは、このオプションおよびアクセス制御方法を説明します。

DNS 権限の決定

DNS セットアップ時にセキュリティー上の予防措置を講じて、ご使用の構成を保護します。どのユーザーが構成変更を許可されているかを設定する必要があります。

ご使用の iSeries の管理者が DNS を構成および管理できるようにする最小レベルの権限が必須です。すべてのオブジェクトのアクセス許可は、管理者が DNS 管理タスクを行うことができることを保証します。DNS を構成予定のユーザーは、全オブジェクト (*ALLOBJ) 権限を持った機密保護担当者とすることをお勧めします。 iSeries ナビゲーターを使用して、ユーザーを許可してください。詳細が必要な場合、DNS オンライン・ヘルプにある「**DNS 管理者への権限の付与**」を参照してください。

注 : 管理者のプロファイルに全権限がない場合、すべての DNS ディレクトリーと関連構成ファイルに対する特定のアクセスと権限が許可されている必要があります。

ドメイン構造の決定

ドメインまたはサブドメインをどのようにゾーン分割するか、ネットワーク要求を最良にサービスし、インターネットにアクセスするにはどうすればよいか、およびファイアウォールのネゴシエーションをどうするかを決定することは重要です。上記の要因は複雑であり、場合に応じて扱い方を代える必要があります。詳細なガイドラインとしては、O'Reilly DNS and BIND 資料などの信頼できる情報源を参照してください。

動的ゾーンとして DNS ゾーンを構成する場合、サーバー稼動中は手動によるゾーン・データへの変更はできません。それを行うと、入ってくる動的更新に悪影響を及ぼします。手動による更新が必要な場合、サーバーを停止し、変更を行ってからサーバーを再始動します。停止した DNS サーバーあてに送信された動的更新は失われます。この理由により、分離して動的ゾーンと静的ゾーンを構成する必要が生じます。 これを行うには、動的に保守される予定のこれらのクライアントに対して、完全に分離したゾーンを作成するか、新規のサブドメイン (dynamic.mycompany.com など) を作成します。

iSeries DNS はグラフィカル・インターフェースを提供して、ご使用のサーバーを構成します。ある場合には、そのインターフェースは、他のソースとは異なる表現の用語または概念を使用する場合があります。DNS 構成計画時に他の情報源を参照する場合、以下のことを知っていると便利です。

- サーバー内で定義されたすべてのゾーンとオブジェクトは、**前方参照ゾーン**と**逆引き参照ゾーン** フォルダー内に作成されています。前方参照ゾーンはドメイン・ネームを IP アドレスにマッピング (A レコードなど) するのに使用するゾーンです。 逆引き参照ゾーンは、IP アドレスをドメイン・ネームにマッピング (PTR レコードなど) するのに使用するゾーンです。
- iSeries DNS は **1 次ゾーン**と **2 次ゾーン**を参照します。他の BIND 資料では、時々「マスター・ゾーン」および「スレーブ・ゾーン」と呼ばれます。
- このグラフィカル・インターフェースでは、**サブゾーン**という用語を使用しますが、一部の他情報源では、サブドメインと呼ぶ場合があります。子ゾーンは、1 つまたは複数のネーム・サーバーにその責任が委譲されたサブゾーンです。

セキュリティー基準の計画

DNS サーバーを保護することは、最重要事項です。以下に示すセキュリティー上の考慮事項に加えて、DNS セキュリティーおよび iSeries セキュリティーについて各種の情報源があります。 (Information Center の IBM Secureway: iSeries とインターネットなど。) DNS and BIND 資料も DNS に関連したセキュリティーを取り扱います。

アドレス・マッチ・リスト

DNS はアドレス・マッチ・リストを使用して、一定の DNS 機能への外部エンティティー・アクセスを許可したり、拒否したりします。このリストには、特定の IP アドレス、サブネット (IP 接頭部を使用)、またはトランザクション・シグニチャー (TSIG) キーの使用を含むことができます。アドレス・マッチ・リストでアクセスを許可または拒否したいエンティティー・リストを定義します。アドレス・マッチ・リストを再使用可能にしたい場合、アクセス制御リスト (ACL) として格納することができます。そうすれば、このリストを提供する必要がある時はいつでも、単に ACL を呼び出して、その完全なリストをロードすることができます。

アドレス・マッチ・リスト要素の順序

指定されたアドレスと一致するアドレス・マッチ・リスト中の最初の要素が使用されます。たとえば、10.1.1.x ネットワーク上の 10.1.1.5 以外の全アドレスを許可するには、この突き合わせリストの要素は (!10.1.1.5; 10.1.1/24) の順序になっている必要があります。この場合、アドレス 10.1.1.5 は最初の要素と比較されて、即時に除外されます。

この要素が (10.1.1/24; !10.1.1.5) のように逆になっていると、IP アドレス 10.1.1.5 はアクセスを許可されてしまいます。理由は、サーバーはそのアドレスを最初の要素と比較し、それが一致すると残りのルールをチェックせずに許可してしまうからです。

アクセス制御オプション
DNS により、制約 (誰がサーバーへの動的更新、照会データ、およびゾーン転送を送信可能か、など) を設定することができるようになります。アクセス制御リストを使用して、サーバーへのアクセスを以下のオプションで制限することができます。

allow-update
ご使用の DNS サーバーが任意の外部ソースからの動的更新を受け入れるためには、allow-update オプションを使用可能にする必要があります。

allow-query
このサーバーへの照会を許可するホストを指定します。この指定がないと、デフォルトが適用され、全ホストからの照会が許可されます。

allow-transfer
このサーバーからのゾーン転送の受信を許可されたホストを指定します。この指定がないと、デフォルトが適用され、全ホストからの転送が許可されます。

allow-recursion
このサーバーを経由して再帰的照会を許可されたホストを指定します。この指定がないと、デフォルトが適用され、全ホストからの再帰的照会が許可されます。

blackhole
サーバーが照会の受け入れを拒否するか、または照会に対応するのに使用しないアドレス・リストを指定します。ここに指定されたアドレスからの照会は応答されません。

DNS システム要件

DNS オプション (オプション 31) は基本オペレーティング・システムと一緒に自動インストールされません。インストール用に DNS を特定して選択する必要があります。 V5R1 で追加された新しい DNS サービスは BIND 8 と呼ばれる業界標準の DNS インプリメンテーションに基づいています。以前の OS/400 DNS サービスは BIND 4.9.3 に基づいていますが、V5R1 でも継続して使用可能です。

いったん、DNS がインストールされると、デフォルトにより、以前のリリースで使用可能だった 4.9.3 ベースの DNS を使用した単一 DNS サーバーをセットアップするように構成されます。 BIND 8 を使用した 1 つまたは複数の DNS サーバーを稼動したい場合は、ポータブル・アプリケーション・ソリューション環境 (PASE) をインストールする必要があります。 PASE は SS1 のオプション 33 です。 PASE がいったんインストールされると、iSeries ナビゲーターが自動的に正しい BIND インプリメンテーションの構成を処理します。

PASE を使用しないと、BIND 8 の機能すべてを利用できるとは限りません。 PASE を使用せずに、BIND 4.9.3 に基づく DNS サーバーを稼動することができます。 PASE を使用しない場合、以前のリリースで使用可能だった DNS サーバー (BIND 4.9.3 ベース) と同じものを継続して実行することができます。V4R5 Information Center にある DNS  を参照してください。

別の iSeries 上の DHCP サーバーを構成して、この DNS サーバーへ更新を送信するようにしたい場合は、オプション 31 を DHCP iSeries にも同様にインストールする必要があります。 DHCP サーバーは、動的更新を行うためにオプション 31 が提供するプログラミング・インターフェースを使用します。

DNS をインストールするかどうかを決定するには、以下のステップに従ってください。
1. コマンド行で「**GO LICPGM**」と入力し、「**Enter**」を押します。

2. 「**10**」(導入済みライセンス・プログラムの表示) と入力して、「**Enter**」を押します。
3. 「**5722SS1 OS/400 - ドメイン・ネーム・システム**」(SS1 のオプション 31) までページ送りします。DNS が正常にインストールされると、以下に示すとおり「**導入状況**」が「***COMPATIBLE**」となります。

```
ライセンス・
プログラム      導入状況        記述
5722SS1         *COMPATIBLE     OS/400 - ドメイン・ネーム・システム
```

4. 「**F3**」を押して表示から出ます。

DNS をインストールするには、以下のステップに従ってください。

1. コマンド行で「**GO LICPGM**」と入力し、「**Enter**」を押します。
2. 「**11**」(ライセンス・プログラムの導入) と入力して「**Enter**」を押します。
3. 「OS/400 - ドメイン・ネーム・システム」の隣の「**オプション**」フィールドに「**1**」(導入) と入力して、「**Enter**」を押します。
4. 「**Enter**」をもう一度押して、インストール結果を再確認します。

DNS 構成

DNS 構成を処理する前に、DNS システム要件を参照して、必要な DNS コンポーネントをインストールします。以下のサブトピックは、ご使用の DNS サーバーを構成するためのガイドラインです。

iSeries ナビゲーターでの DNS のアクセス方法
iSeries ナビゲーターで DNS をアクセスするための手順が説明されています。

ネーム・サーバーの構成
DNS により複数ネーム・サーバー・インスタンスを作成できるようになります。 このトピックではネーム・サーバーの構成手順を説明します。

動的更新を受信するための DNS の構成方法
BIND 8 で稼動する DNS サーバーは、ゾーン・データを動的に更新するため他ソースからの要求を受け入れるように構成することができます。このトピックでは、allow-update オプションの構成手順を説明します。それにより、DNS が動的更新を受信できるようになります。

DNS ファイルのインポート
DNS は既存のゾーン・データ・ファイルをインポートすることができます。既存構成ファイルから新しいゾーンを作成するために、上記の時間のかからない手順に従ってください。

外部 DNS データ・アクセス
DNS ゾーン・データを作成すると、ご使用のサーバーはそのゾーンに対するアドレス照会に回答できます。このトピックでは、自分自身のドメインの外部のアドレス照会に応答する DNS 構成方法を説明します。

iSeries ナビゲーターでの DNS のアクセス方法

以下の手順では、iSeries ナビゲーターで DNS 構成インターフェースに進みます。 PASE を使用している場合、BIND 8 に基づく DNS サーバーを構成することができます。 PASE を使用しない場合、以前のリリースで使用可能だった DNS サーバー (BIND 4.9.3 ベース) と同じものを継続して実行することができます。BIND 4.9.3 ベースの DNS 関連情報については、V4R5 Information Center にある DNS  を参照してください。

初めて DNS を構成する場合、以下の手順に従ってください。

1. **iSeries ナビゲーター**で、**使用する iSeries サーバー** —>「**ネットワーク**」—>「**サーバー**」—>「**DNS**」と展開します。
2. 「**DNS**」を右クリックして「**新規ネーム・サーバー**」を選択します。

V5R1 より前の DNS サーバーを構成済みの場合、以下のステップに従ってください。

1. **iSeries ナビゲーター**で、**使用する iSeries サーバー** —>「**ネットワーク**」—>「**サーバー**」—>「**DNS**」と展開します。
2. 右側のペインで DNS サーバーをダブルクリックして「**DNS 構成**」ウィンドウを開きます。
3. PASE を使用している場合、既存の DNS 構成を BIND 8 をインプリメントした構成にマイグレーションするオプションが提供されます。ただし、いったん BIND 8 にマイグレーションすると、BIND 4.9.3 へは逆戻りできません。どうすればよいか分からない場合は、「**No**」を選択してください。マイグレーションしたい場合は「**Yes**」を選択します。
4. 好きな時に DNS サーバーを BIND 8 にマイグレーションするには、左側のペインで「**DNS**」を右クリックし「**バージョン 8 に移行**」を選択します。

ネーム・サーバーの構成

iSeries DNS (BIND 8 ベース) は複数ネーム・サーバー・インスタンスをサポートします。以下に示す作業では、そのプロパティーおよびゾーンを含む単一ネーム・サーバー・インスタンスの作成のプロセスを行います。

1. ネーム・サーバー・インスタンスの作成
   「**新規 DNS 構成**」ウィザードを使用して、DNS サーバー・インスタンスを定義します。
2. DNS サーバー・プロパティーの編集
   ご使用の新しいサーバー・インスタンス用のグローバル・プロパティーを定義します。
3. ネーム・サーバー上のゾーン構成
   ご使用のネーム・サーバーを入れるゾーンとゾーン・データを作成します。

複数インスタンスを作成したい場合、必要なすべてのインスタンスが作成されるまで、上記の手順を繰り返してください。各ネーム・サーバー・インスタンスごとに、デバッグ・レベルおよび自動開始値などの独立したプロパティーを指定することができます。新しいインスタンスが作成されると、個別の構成ファイルが作成されます。構成ファイルの詳細は、DNS 構成ファイルの維持管理を参照してください。

ネーム・サーバー・インスタンスの作成

「**New DNS Configuration**」ウィザードを開始するには、以下のステップに従ってください。

1. **iSeries ナビゲーター**で、**使用する iSeries サーバー** —>「**ネットワーク**」—>「**サーバー**」—>「**DNS**」と展開します。
2. 左側のペインで「**DNS**」を右クリックし、「**新規ネーム・サーバー**」を選択します。
3. このウィザードが構成プロセスをガイドします。

このウィザードには以下の入力が必要です。

DNS サーバー名 : DNS サーバー用の名前を入力します。この名前は 5 文字までの長さで、英字で始まっている必要があります。複数サーバー作成時は、各名前は固有である必要があります。この名前は、システムの他のエリアで DNS サーバー「インスタンス」名と呼ばれます。

IP アドレスの listen : 2 つの DNS サーバーは、同一 IP アドレスを listen-on することはできません。デフォルト設定では、すべてを listen-on します。追加のサーバー・インスタンスを作成する場合、すべての IP アドレスを listen-on するように構成することはできません。各サーバーごとに IP アドレスを指定する必要があります。

ルート・サーバー : デフォルトのインターネット・ルート・サーバーか、またはイントラネット用の内部ルート・サーバーなど、自分自身のルート・サーバー・リストをロードしても構いません。
注 : インターネットを使用していて、ご使用の DNS がインターネット名を完全に解決できることを期待している場合、デフォルトのインターネット・ルート・サーバーをロードすることだけを考慮する必要があります。

サーバーの開始 : TCP/IP 始動時に、サーバーが自動開始すべきかどうかを指定することができます。複数サーバーを稼動する場合、個々のインスタンスはお互いに無関係に開始および終了することができます。

次の作業項目 : DNS サーバー・プロパティーの編集。

DNS サーバー・プロパティーの編集

ネーム・サーバー作成後、allow-update やデバッグのレベルなどのプロパティーを編集することができます。これらのオプションは、変更しようとするサーバー・インスタンスにのみ適用されます。 DNS サーバー・インスタンスのプロパティーを編集するには、以下のステップに従ってください。

1. **iSeries ナビゲーター**で、**使用する iSeries サーバー** —>「**ネットワーク**」—>「**サーバー**」—>「**DNS**」と展開します。
2. 右側のペインで**使用する DNS サーバー**を右クリックし、「**構成**」を選択します。
3. 「**DNS サーバー**」を右クリックし、「**プロパティー**」を選択します。

次の作業項目 : ネーム・サーバー上のゾーンの構成。

ネーム・サーバー上のゾーンの構成

いったん、ネーム・サーバーが作成されると「**iSeries ナビゲーター**」メイン・ウィンドウに戻ります。ご使用のサーバーは右側のペインに表示されます。ご使用のサーバー上にゾーンを構成するには、サーバー名を右クリックして、「**構成**」を選択します。「**DNS 構成**」ウィンドウが表示されます。

すべてのゾーンはウィザードを使用して構成されます。関連するフォルダーを右クリックして「**前方参照ゾーン**」または「**逆引き参照ゾーン**」を作成します。そのゾーン・タイプ用のオプションが表示されます。作成したいゾーン・タイプを選択して、ウィザードを開始します。

V5R1 DNS で作成可能なオブジェクト・タイプの説明は、DNS についてを参照してください。

いったん、ご使用のゾーンが構成されると、詳細な構成情報用に以下のトピックを参照する必要がでてきます。

動的更新を受け入れるためのゾーン構成方法
動的更新により、許可されたソースがリソース・レコードを送信してゾーン・データを更新できるようになります。これにより、手作業でゾーン・データを変更する必要性が減少します。

ゾーン・データのインポート
別の DNS サーバーで既存のゾーン・データ・ファイルがある場合、ご使用の新規サーバーにそれをアップロードすることができます。

外部 DNS データ・アクセス
ご使用のサーバーを構成して、そのサーバーに含まれるゾーン・データの外部にある情報に対して照会に対応する必要が生じます。照会を他の許可サーバーに転送するか、または照会を解決するのに有効なルート・サーバーをロードすることができます。

動的更新を受信するための DNS の構成方法

動的ゾーン作成時、ネットワーク構造を考慮する必要があります。ドメインの一部がまだ手動による更新を必要とする場合、分離された静的ゾーンと動的ゾーンをセットアップすることができます。動的ゾーンに対して手動による更新を行う場合、動的ゾーンのサーバーを停止して、更新完了後に再始動する必要があります。サーバーを停止することは、サーバーがゾーン・データベースからゾーン・データをロードした時点以降に行った、すべての動的更新を強制的に同期化することを意味します。サーバーを停止しなかった場合、サーバーが最後に開始して以来、処理されたすべての動的更新は失われます。ただし、サーバーを停止して手動による更新を行った場合、サーバーが停止中に発生した動的更新は失われます。

オブジェクトが allow-update ステートメントで定義されていると、DNS はゾーンが動的であることを示します。 allow-update オプションを構成するには、以下のステップに従ってください。

1. **iSeries ナビゲーター**で、**使用する iSeries サーバー** —>「**ネットワーク**」—>「**サーバー**」—>「**DNS**」と展開します。
2. 右側のペインで**使用する DNS サーバー**を右クリックし、「**構成**」を選択します。
3. 「**DNS 構成**」ウィンドウで、「**前方参照ゾーン**」または「**逆引き参照ゾーン**」を画面展開してください。
4. 編集したい 1 次ゾーンを右クリックして「**プロパティー**」を選択します。
5. 「**1 次ゾーン・プロパティー**」ページで「**オプション**」タブをクリックします。
6. 「**オプション**」ページで「**アクセス制御**」—>「**allow-update**」の順に画面展開します。
7. DNS はアドレス・マッチ・リストを使用して、許可された更新を検証します。アドレス・マッチ・リストにオブジェクトを追加するには、アドレス・マッチ・リストの要素タイプを選択し「**追加**」をクリックすると、IP アドレス、IP 接頭部、アクセス制御リスト、またはキーを追加できます。
8. アドレス・マッチ・リストの更新終了後「**OK**」をクリックして、「**オプション**」ページを閉じます。

iSeries DHCP サーバーからの動的更新を受信するように DNS をセットアップするには、動的更新を送信するための DHCP の構成を参照してください。

DNS ファイルのインポート

ゾーン・データ・ファイルをインポートするか、または既存のホスト・テーブルを変換することによって 1 次ゾーンを作成することができます。ホスト・テーブルからゾーン・データを作成するには、V4R5 Information Center にある ホスト・テーブルの変換  を参照してください。

BIND 構文に基づく有効なゾーン構成ファイルであれば、任意のファイルをインポートできます。このファイルは IFS ディレクトリーに配置する必要があります。インポートされた場合、DNS はそれが有効なゾーン・データ・ファイルであることを確認して、ゾーン・データ・ファイルをこのサーバー・インスタンス用の NAMED.CONF ファイルに追加します。

ゾーン・ファイルをインポートするには、以下のステップに従ってください。

1. **iSeries ナビゲーター**で、**使用する iSeries サーバー** —>「**ネットワーク**」—>「**サーバー**」—>「**DNS**」と展開します。
2. 右側のペインで、ゾーンをインポートしたい DNS サーバー・インスタンスをダブルクリックします。

3. 左側のペインで「**DNS サーバー**」を右クリックし、「**ゾーンのインポート**」を選択します。
4. ウィザードの指示に従って、1 次ゾーンをインポートします。

レコードの妥当性検査

ドメイン・データ・インポート機能は、インポート予定のファイルの各レコードを読み込んで妥当性検査します。ドメイン・データ・インポート機能が完了すると、エラーとなったすべてのレコードが、インポートされたゾーンの「**別のレコード**」プロパティー・ページ上で個々に調べられます。

- **注 :**
- 大規模な 1 次ドメインをインポートすると、数分かかる場合があります。
- ドメイン・データ・インポート機能は $include ディレクティブをサポートしません。ドメイン・データ・インポート機能の妥当性検査プロセスは、エラーのある行と同様に、$include ディレクティブを含んだ行を識別します。

外部 DNS データ・アクセス

ルート・サーバーは、インターネットまたは大規模イントラネットに直接接続している DNS サーバーの機能にとって非常に重要です。DNS サーバーは、ルート・サーバーを使用して、自分のドメイン・ファイル中に入っているホスト以外のホストに関する照会に応答する必要があります。

詳しい情報を得るためには、DNS サーバーはどこを探せばよいかを知っている必要があります。インターネット上で、DNS サーバーが最初に探す場所がルート・サーバーです。 ルート・サーバーは、照会への応答が見付かるか応答できないと分かるまで、DNS サーバーに階層の他のサーバーへの経路を指示します。

iSeries ナビゲーターのデフォルト・ルート・サーバー・リスト

インターネット・ルート・サーバーは、インターネット接続があり、かつ自分の DNS サーバーでは解決できない時にインターネット上で名前を解決したい場合に限って、使用してください。インターネット・ルート・サーバーのデフォルト・リストは、iSeries ナビゲーターにあります。そのリストは、iSeries ナビゲーターがリリースされた時点のものです。このデフォルト・リストを InterNIC サイト上のリストと比較して、デフォルト・リストが最新版であるかを確認することができます。ご使用の構成のルート・サーバー・リストが常に最新状態になるように更新してください。

インターネットのルート・サーバー・アドレスの入手先

階層の最上位にあるルート・サーバーのアドレスは時々刻々変化します。これを最新状態に保っておく責任は管理者にあります。 InterNIC はインターネットのルート・サーバー・アドレスの最新リストを保守します。インターネットのルート・サーバー・アドレスの最新リストを入手するには、以下の手順に従ってください。

1. InterNIC サーバー `FTP.RS.INTERNIC.NET` に匿名の FTP を行います。
2. 次のファイルをダウンロードします。`/domain/named.root`
3. そのファイルを次のディレクトリー・パスに格納します。**統合ファイル・システム**
   `/Root/QIBM/ProdData/OS400/DNS/ROOT.FILE`

ファイアウォールの後ろ側にある DNS には、ルート・サーバーが定義されていない場合があります。この場合、DNS サーバーは、それ自身の 1 次ドメイン・データベース・ファイルまたはキャッシュに存在するエントリーからのみ、照会を解決することができます。このサーバーはオフサイト照会をファイアウォール DNS に転送する場合があります。この場合、ファイアウォール DNS サーバーは転送者のように機能します。

イントラネット・ルート・サーバー

ご使用の DNS サーバーが大規模イントラネットの一部の場合、内部ルート・サーバーを持つ場合がありま

す。ご使用の DNS サーバーがインターネットにアクセスしない場合は、デフォルトのインターネット・サーバーをロードする必要はありません。ただし、ご使用の DNS サーバーがそのドメイン外の内部アドレスを解決できるように、内部ルート・サーバーを追加する必要があります。

DNS 管理

いったん DNS が構成されると、以下のトピックを検討する必要があります。

NSLookup による DNS 機能の検証
NSLookup を使用して DNS が機能しているかどうか検証できます。

セキュリティー・キー管理
セキュリティー・キーにより、ご使用の DNS データへのアクセスを制限できるようになります。

DNS サーバー統計
データベース・ダンプおよび統計ツールは、サーバーのパフォーマンスを検討および管理するのに有効です。

DNS 構成ファイルの維持管理
DNS が使用するファイルを理解し、そのファイルをバックアップおよび保守するためのガイドラインを説明します。

拡張 DNS オプション
このトピックでは、経験のある管理者がどのようにして拡張機能にアクセスできるかを説明します。

NSLookup による DNS 機能の検証

DNS サーバーを IP アドレスで照会するために、NSLookup (ネーム・サーバー検索) を使用します。これにより、DNS が照会に応答できるかどうかを検証します。ループバック IP アドレス (127.0.0.1) に関連したホスト名を要求します。ホスト名 (localhost) で応答される必要があります。検証しようとするサーバー・インスタンスに定義された特定の名前も照会する必要があります。これにより、テストしている特定サーバー・インスタンスが正しく機能していることを確認できます。

NSLookup で DNS 機能を検証するには、以下のステップに従ってください。

1. コマンド行で「NSLOOKUP DMNNAMSVR(n.n.n.n)」と入力します。ここで、n.n.n.n は、テストで listen-on する構成済みのサーバー・インスタンスのアドレスです。
2. コマンド行で「NSLOOKUP」と入力し、「**Enter**」を押します。これにより、NSLookup 照会セッションが開始します。
3. ご使用のサーバー名の前に「server」と入力して、「**Enter**」を押します。たとえば「server myiseries.mycompany.com」のように入力します。
   この結果、以下のように表示されます。

   ```
   サーバー:  myiseries.mycompany.com
   アドレス: n.n.n.n
   ```

   ここで、n.n.n.n はご使用の DNS サーバーの IP アドレスを意味します。
4. コマンド行で「127.0.0.1」と入力し、「**Enter**」押します。
   この結果、ループバック・ホスト名を含んで、以下の情報が表示されます。

```
 > 127.0.0.1
サーバー:  myiseries.mycompany.com
アドレス:  n.n.n.n

名前:    localhost
アドレス:  127.0.0.1
```

DNS サーバーがループバック・ホスト名「**localhost**」を戻した場合は、その DNS サーバーは正しく応答しています。

5. 「exit」と入力し、「**Enter**」を押して NSLOOKUP 端末セッションを終了します。

注： NSLookup 使用上でヘルプが必要な場合は「?」と入力してください。そして「**Enter**」を押します。

セキュリティー・キー管理

DNS に関連する 2 つのタイプのキーがあります。この各キーはご使用の DNS 構成を保護する上で異なる役割を果たします。以下に、各キーが DNS サーバーにどのように関連するかを説明します。

DNS キー

DNS キーは BIND に対して定義されたキーです。このキーは、入ってくる更新の検証処理の一部として DNS サーバーにより使用されます。キーを構成し、それに名前を付けることができます。それから、DNS オブジェクト (動的ゾーンなど) を保護したい場合、Address Match List 中にキーを指定できます。

DNS キーを管理するには、以下のステップに従ってください。

1. **iSeries ナビゲーター**で、**使用する iSeries サーバー** —>「**ネットワーク**」—>「**サーバー**」—>「**DNS**」と展開します。
2. 右側のペインで、オープンしたい DNS サーバー・インスタンスを右クリックし、「**構成**」を選択します。
3. 「**DNS 構成**」ウィンドウで、「**ファイル**」—>「**キーの管理**」を選択します。

動的更新キー

動的更新キーは、DHCP による動的更新を保護するのに使用します。このキーは DNS と DHCP が同一 iSeries 上にある場合に必要になります。DHCP が別の iSeries にある場合は、各 iSeries サーバー上に同じ動的更新キーを作成して、動的更新の保護ができるようにする必要があります。

動的更新キーを管理するには、以下のステップに従ってください。

1. **iSeries ナビゲーター**で、**使用する iSeries サーバー** —>「**ネットワーク**」—>「**サーバー**」—>「**DNS**」と展開します。
2. 「**DNS**」を右クリックし「**動的更新キーの管理**」を選択します。

DNS サーバー統計

DNS はいくつかの診断ツールを提供します。サーバーのパフォーマンスをモニターするのに使用できます。

サーバー統計

DNS により、サーバー・インスタンスに対する統計を表示できるようになります。これらの統計は、サーバーが最後に再始動したか、またはそのデータベースを再ロードして以降、そのサーバーが受信した照会と応答の数を要約します。統計情報は継続的にこのファイルに追加され、このファイルが削除されるまで続きます。この情報は、どの程度のトラフィックをサーバーが受信しているかの評価、および障害によるダウンの発生のトラッキングに有効です。サーバー統計の詳細は、DNS のオンライン・ヘルプ・トピックの**DNS サーバー統計**で入手可能です。

サーバー統計にアクセスするには、以下のステップに従ってください。

1. **iSeries ナビゲーター**で、**使用する iSeries サーバー** —>「**ネットワーク**」—>「**サーバー**」—>「**DNS**」と展開します。
2. 右側のペインで**使用する DNS サーバー**を右クリックし、「**構成**」を選択します。
3. 「**DNS 構成**」ウィンドウで、「**表示**」—>「**サーバー統計**」を選択します。

アクティブ・サーバー・データベース

DNS により、許可データ、キャッシュ・データ、およびサーバー・インスタンスに対する障害判別のヒントとなるデータのダンプを表示できるようになります。 このダンプには、サーバーが照会から入手した情報と、すべてのサーバーの 1 次および 2 次ゾーン (順および逆マッピング・ゾーン) からの情報が含まれています。このデータベースには、ゾーンとホスト情報が含まれています。この情報には、一部のゾーン・プロパティー (許可の開始 (SOA) 情報など) および全ホスト・プロパティー (メール・エクスチェンジャー (MX) 情報など) が含まれています。この情報は、障害によるダウン発生をトラッキングするのに有効です。

iSeries ナビゲーターを使用して、アクティブ・サーバー・データベースのダンプを表示できます。このファイルのコピーを保管する必要がある場合、そのデータベース・ダンプ・ファイルの名前は、NAMED_DUMP.DB であり、iSeries ディレクトリー・パス (**統合ファイル・システム /Root/QIBM/UserData/OS400/DNS/<server instance>**) にあります。ここで、“<server instance>” は DNS サーバー・インスタンス名です。アクティブ・サーバー・データベースの詳細は、DNS のオンライン・ヘルプ・トピックの「**DNS サーバー・データベース・ダンプの理解**」で入手可能です。

アクティブ・サーバー・データベース・ダンプにアクセスするには、以下のステップに従ってください。

1. **iSeries ナビゲーター**で、**使用する iSeries サーバー** —>「**ネットワーク**」—>「**サーバー**」—>「**DNS**」と展開します。
2. 右側のペインで**使用する DNS サーバー**を右クリックし、「**構成**」を選択します。
3. 「**DNS 構成**」ウィンドウで、「**表示**」—>「**アクティブ・サーバー・データベース**」を選択します。

DNS 構成ファイルの維持管理

OS/400 DNS を使用して、iSeries 上の DNS サーバー・インスタンスを作成および管理することができます。 DNS 用の構成ファイルは iSeries ナビゲーターにより管理されます。このファイルは、手動で編集しないでください。必ず iSeries ナビゲーターを使用して、DNS 構成ファイルの作成、変更、または削除を行ってください。 DNS 構成ファイルは、以下にリストされた統合ファイル・システムのパスに保管されます。

注: 以下のファイル構造は BIND 8 上で実行する DNS に適用されます。BIND 4.9.3 ベースの DNS を使用している場合、V4R5 DNS Information Center トピックにある DNS 構成ファイルのバックアップとログ・ファイルの保守 を参照してください。

以下の表には、各ファイルがパスの階層順にリストされています。保管アイコン の付いたファイルは、データを保護するためバックアップをとってください。削除アイコン の付いたファイルは定期的に削除してください。

名前		説明
QIBM/UserData/OS400/DNS/		DNS 用の開始点ディレクトリー

名前		説明
ATTRIBUTES		DNS はこのファイルを使用して、どのバージョンの BIND を使用しているかを判別します。
QIBM/UserData/OS400/DNS/*<instance-n>*/		DNS インスタンス用の開始点ディレクトリー
ATTRIBUTES		iSeries DNS により使用される構成属性
NAMED.CONF		このファイルには構成データが含まれます。サーバーに管理する特定ゾーン、ゾーン・ファイルの場所、動的に更新されるゾーン、転送先サーバーの場所、およびその他のオプション設定を知らせるのに使用されます。
BOOT.AS400BIND4		BIND 4.9.3 サーバー構成およびポリシー・ファイル。このファイルはこのインスタンス用の BIND 8 NAMED.CONF ファイルへ変換されます。このファイルは、BIND 4.9.3 サーバーを BIND 8 にマイグレーションする場合に作成されます。このファイルは、マイグレーション用のバックアップとして機能し、BIND 8 が正常に作動すれば削除しても構いません。
NAMED.CA		このサーバー・インスタンス用のルート・サーバー・リスト。
NAMED_DUMP.DB		アクティブ・サーバー・データベース用に作成されたサーバー・データ・ダンプ。
NAMED.STATS		サーバー統計。
NAMED.PID		実行中サーバーの Process ID を保持。このファイルは、DNS サーバーが始動するたびに、作成されます。このファイルは、データベース、統計、および更新サーバー用に使用されます。このファイルは編集または削除しないでください。
QUERYLOG		受信した照会の DNS サーバー・ログ。このファイルは、DNS サーバー・ログがアクティブになると、作成されます。アクティブ時は、このファイルは大きくなるため、定期的に削除する必要があります。
<*zone-name-a*>.DB		このサーバーが提供する特定ドメイン用のゾーン・ファイル。このゾーン用のリソース・レコードすべてが含まれます。

名前		説明
<*zone-name-b*>.DB		このサーバーが提供する特定ドメイン用のゾーン・ファイル。このゾーン用のリソース・レコードすべてが含まれます。各ゾーンには個別の .DB ファイルがあります。
.ixfr.		増分ゾーン転送 (IXFR) ファイル。このファイルは 2 次サーバーが使用して、最後のゾーン転送以降に発生した変分データのみロードします。更新が行われると、IXFR ファイルの数が増加します。古い IXFR ファイルは定期的に削除してください。過去 1 ～ 2 日内に作成されたファイルを残しておくと、ほとんどの 2 次サーバーが引き続き IXFR をロードできます。このファイルのすべてを削除すると、2 次サーバーは完全転送 (AXFR) を要求します。
TMP		一時的作業ファイルの作成用に、サーバー・インスタンスが使用するディレクトリー。
QIBM/UserData/OS400/DNS/TMP		QTOBH2N プログラムが使用する一時的なディレクトリー。QTOBH2N プログラムは iSeries ナビゲーターにより後でインポートするために、ホスト・テーブルからダンプされた中間ファイルを作成します。
QIBM/UserData/OS400/DNS/_DYN/		動的更新に必須のファイルを保持するディレクトリー。
<*key_id-name-x*>._KID		<*key_id-name-x*> という名の key_id で、BIND 8 キー・ステートメントを含むファイル。
<*key_id-name-x*>._DUK.<*zone-name-a*>		<*key_id-name-x*> キーを使用して、<*zone-name-a*> への動的更新要求を開始するのに必要な動的更新キー。
<*key_id-name-y*>._KID		<*key_id-name-y*> という名の key_id で、BIND 8 キー・ステートメントを含むファイル。
<*key_id-name-y*>._DUK.<*zone-name-a*>		<*key_id-name-y*> キーを使用して、<*zone-name-a*> への動的更新要求を開始するのに必要な動的更新キー。
<*key_id-name-y*>._DUK.<*zone-name-b*>		<*key_id-name-y*> キーを使用して、<*zone-name-b*> への動的更新要求を開始するのに必要な動的更新キー。

拡張 DNS 機能

iSeries ナビゲーターの中で DNS は、DNS サーバーを構成および管理するためのインターフェースを提供します。以下のタスクがショートカットとして、iSeries グラフィカル・インターフェースに精通した管理者に提供されます。このインターフェースは、複数インスタンスのサーバー状況および属性を一度に変更するための、迅速な方法を提供します。

DNS 属性の変更

DNS インターフェースは、すべてのサーバー・インスタンスの自動開始とデバッグ・レベルを一度に変更することを許可しません。文字ベースのインターフェースを使用して個別に DNS サーバー・インスタンスに対してこれらの設定を変更するか、または一度にすべてのインスタンスに対して変更することができます。CHGDNSA を使用する以下のステップに従ってください。

1. コマンド行で「CHGDNSA」と入力して、「**F4**」を押します。
2. 「DNS サーバー属性の変更」(CHGDNSA) ページ上で、単一サーバー・インスタンスか、または「*ALL」と入力して「**Enter**」を押します。

   以下の、使用可能なサーバー・オプションが表示されます。

   ```
   自動開始サーバー . . . . . *SAME *YES, *NO, *SAME
   デバッグ・レベル . . . . . *SAME 0-11, *SAME, *DFT
   ```

3. **自動開始** 選択された DNS サーバーが TCP/IP 始動時に自動開始するように指定するには、「*YES」と入力してください。 TCP/IP 始動時にサーバーを自動開始させたくない場合は、「*NO」の入力してください。現行の設定のままで属性を残したい場合は「*SAME」と入力してください。

   デバッグ・レベル 選択されたサーバーが使用するデバッグ・レベルを変更するには、0 ～ 11 の値を入力します。サーバー始動時のデバッグ・レベルを引き継いで使用したい場合は「*DFT」と入力します。現行の設定のままで属性を残したい場合は「*SAME」と入力してください。

   すべてのプリファレンスを入力完了後は「**Enter**」を押して、DNS 属性を設定します。

DNS サーバーの始動と停止

DNS インターフェースは、すべてのサーバー・インスタンスを一度に始動または停止することを許可しません。文字ベースのインターフェースを使用して複数インスタンスに対するこの設定を一度に変更することができます。文字ベースのインターフェースを使用してすべての DNS サーバー・インスタンスを一度に始動するには、コマンド行で「STRTCPSVR SERVER(*DNS) DNSSVR(*ALL)」と入力してください。一度にすべての DNS サーバー を停止するには、コマンド行で「ENDTCPSVR SERVER(*DNS) DNSSVR(*ALL)」と入力してください。

デバッグ値の変更

iSeries Navigator インターフェースで DNS は、稼動中サーバーのデバッグ・レベルを変更することを許可しません。ただし、文字ベースのインターフェースを使用して、稼動中サーバーのデバッグ・レベルを変更できます。この機能は、大規模ゾーンを持ち、大量のデバッグ・データ (サーバーが最初に始動して、そのゾーン・データすべてをロードしている間に入手されたデータ) が不要な管理者にとって有効です。文字ベースのインターフェースを使用してデバッグ・レベルを変更するには、以下のステップに従って、<instance> をサーバー・インスタンス名で置き換えてください。

1. コマンド行で「ADDLIBLE QDNS」と入力して「**Enter**」を押します。
2. デバッグ・レベルを以下のようにして変更します。
   - デバッグをオンにするか、またはデバッグ・レベルを 1 ずつ増やすには、「CALL QTOBDRVS ('BUMP' '<instance>')」と入力して「**Enter**」を押します。
   - デバッグをオフにするには、「CALL QTOBDRVS ('OFF' '<instance>')」と入力して「**Enter**」を押します。

DNS のトラブルシューティング

DNS は、他の TCP/IP 機能およびアプリケーションとほぼ同じ機能をします。DNS ジョブは、SMTP または FTP アプリケーションと同じように、QSYSWRK サブシステムのもとで実行され、それによって、この DNS ジョブに関連した情報を含むジョブ・ログを、ユーザー・プロファイル QTCP の下に作成します。DNS ジョブが終了すると、原因を判別するためにそのジョブ・ログを使用できます。DNS サーバーが期待していた応答を戻さない場合、ジョブ・ログに問題分析に役立つ情報が含まれていることがあります。

DNS 構成は、異なるタイプのレコードが入っている複数のファイルによって構成されます。DNS サーバーの問題は、一般には DNS 構成ファイルのエントリーが誤っていることが原因です。問題が生じたときには、DNS 構成ファイルに期待どおりのエントリーになっているか確認してください。

ロギング
DNS は膨大なロギング・オプションを提供し、問題の原因追及時はそのオプションを調整することができます。ロギングには、各種の重大度レベル、メッセージ・カテゴリー、および出力ファイルを提供することにより、柔軟性があります。それにより、ロギングを正しくチューニングして問題発見に役立ちます。

デバッグ設定
DNS は 12 レベルでデバッグをコントロールします。ロギングは、通常、容易に問題を発見する方法を提供しますが、ある場合には、デバッグすることが必要となる場合があります。通常の状態では、デバッグはオフ (値を 0 にする) にします。

その他のトラブルシューティング・リソース
DNS の一般的なトラブルシューティング情報は多くのソースから入手可能です。 特に「O'Reilly DNS and BIND」資料は一般的な質問に対してよい回答が参照でき、DNS リソース・ディレクトリーは DNS 管理者のために検討グループへのリンクを提供します。

ジョブの識別
ジョブ・ログの中を探して DNS サーバー機能 (たとえば、WRKACTJOB の使用) を検証したい場合、以下に示すガイドラインを検討してください。

- BIND 4.9.3 を使用している場合、サーバーのジョブ名は QTOBDNS となります。 DNS 4.9.3 のデバッグに関する詳細は、V4R5 TCP/IP 構成および解説書 にある、DNS トラブルシューティングを参照してください。
- BIND 8 ベースのサーバーを稼動している場合、稼動しているサーバー・インスタンスごとに個別のジョブがあります。ジョブ名は 5 文字 (QTOBD) 固定で、インスタンス名が続きます。たとえば、INST1 と INST2 の 2 つのインスタンスがある場合、そのジョブ名は QTOBDINST1 と QTOBDINST2 となります。

DNS サーバー・ロギング

BIND 8 はいくつかの新しいロギング・オプションを提供します。ログに記録するメッセージ・タイプ、各メッセージ・タイプの送信先、およびログに記録する各メッセージ・タイプの重大度を指定できます。一般に、デフォルトのロギング設定をそのまま適用しても構いませんが、設定を変更したい場合、ロギングについて、BIND 8 に関するその他の情報を参照することをお勧めします。

ロギング・チャネル
DNS サーバーは別の出力チャネルに、メッセージをログに記録することができます。チャネルはログ・データの送信先を指定します。以下のチャネル・タイプを選択できます。

- **ファイル・チャネル**
  ファイル・チャネルにログ記録されるメッセージはファイルに送信されます。デフォルトのファイル・チャネルは、as400_debug と as400_QPRINT です。デフォルトにより、デバッグ・メッセージは as400_debug チャネルにログ記録されます。これは NAMED.RUN ファイルです。しかし、他のメッセージ・カテゴリーも同様にこのファイルに送信することができます。 as400_QPRINT にログ記録されるメッセージ・カテゴリーは、ユーザー・プロファイル QTCP 用の QPRINT スプール・ファイルに送信されます。提供されたデフォルトのチャネルの他に、自分自身のファイル・チャネルを作成できます。
- **Syslog チャネル**
  このチャネルにログ出力されたメッセージは、サーバーのジョブ・ログに送信されます。デフォルトの syslog チャネルは as400_joblog です。このチャネルにルーティングされたロギング・メッセージは、DNS サーバー・インスタンスのジョブ・ログに送信されます。
- **ヌル・チャネル**
  ヌル・チャネルにログ記録された全メッセージは廃棄されます。デフォルトのヌル・チャネルは as400_null です。どのログ・ファイルにもメッセージを出力したくない場合、ヌル・チャネルにカテゴリーをルーティングすることができます。

メッセージ・カテゴリー
メッセージはカテゴリーにグループ化されます。各チャネルにログ記録されるメッセージ・カテゴリーを指定することができます。以下のような、多くのカテゴリーがあります。

- config: 構成ファイル処理
- db: データベース操作
- queries: サーバーが受信する各照会に対する短いログ・メッセージを生成
- lame-servers: 間違った照会代行の検知
- update: 動的更新
- xfer-in: サーバーが受信しているゾーン転送
- xfer-out: サーバーが送信しているゾーン転送

ログ・ファイルは大きくなるため、定期的に削除する必要があります。すべての DNS サーバーのログ・ファイルは、DNS サーバーを停止して始動するとクリアされます。

メッセージ重大度
チャネルは、メッセージ重大度によりメッセージをフィルターに掛けることができます。各チャネルごとに、メッセージがログ出力される重大度レベルを指定することができます。以下に、使用可能な重大度レベルを示します。

- 重大
- エラー
- 警告
- 注意
- 情報のみ
- デバッグ (デバッグ・レベル 0 ～ 11 を指定)
- 動的 (サーバー始動時のデバッグ・レベルを引き継ぐ)

上記リスト中で選択した重大度および指定したレベルより高い重大度レベルを持つすべてのメッセージがログに記録されます。たとえば、警告を選択した場合、チャネルは警告、エラー、および重大メッセージをログに記録します。デバッグ・レベルを選択した場合、デバッグ・メッセージをログ出力したい 0 ～ 11 の値を指定できます。

ログ設定の変更

ロギング・オプションにアクセスするには、以下のステップに従ってください。

1. **iSeries ナビゲーター**で、**使用する iSeries サーバー** —>「**ネットワーク**」—>「**サーバー**」—>「**DNS**」と展開します。
2. 右側のペインで**使用する DNS サーバー**を右クリックし、「**構成**」を選択します。
3. 「**DNS 構成**」ウィンドウで「**DNS サーバー**」を右クリックし、「**プロパティー**」を選択します。
4. 「**サーバー・プロパティー**」ウィンドウで「**チャネル**」タブを選択します。これは、新規のファイル・チャネルまたはチャネルのプロパティー (各チャネルに対してログに記録されるメッセージ重大度など) を作成するためです。
5. 「**サーバー・プロパティー**」ウィンドウで、「**ロギング**」タブを選択します。これは、どのメッセージ・カテゴリーが各チャネルにログ出力されるかを指定するためです。

トラブルシューティングのヒント

as400_joblog チャネルのデフォルト重大度レベルは、エラーに設定されています。この設定により、情報のみレベル、および警告レベルのメッセージの量を減少させるのに使用されます。そうしないと、パフォーマンスの低下を起こす可能性があります。問題が発生して、その問題の原因がジョブ・ログに示されていない場合、重大度レベルを変更する必要があります。上記の手順に従って「チャネル」ページにアクセスし、as400_joblog チャネル用重大度レベルを、警告、注意、または情報のみのいずれかに変更してください。そうすれば、より多くのログ・データを表示することができます。それにより問題が解決した後は、重大度レベルをエラーに戻してジョブ・ログに出力されるメッセージ数を減少させます。

DNS デバッグ設定

DNS デバッグ機能は、DNS サーバー上の問題を判別および修正するのに有効な情報を提供します。まず最初にロギングを使用して問題修正を試みることをお勧めします。

有効なデバッグ・レベルは、0 ～ 11 です。IBM サービス技術員は、DNS の問題を診断するのに適切なデバッグ値を決定するためのサポートを行うことができます。 1 またはそれ以上の値は、デバッグ情報を、iSeries ディレクトリー・パス (**統合ファイル・システム/Root/QIBM/UserData/OS400/DNS/<server instance>**) にある NAMED.RUN ファイルに出力します。ここで、“<server instance>” は DNS サーバー・インスタンス名です。NAMED.RUN ファイルは、デバッグ・レベルが 1 またはそれ以上に設定されて DNS が実行され続ける限り、増え続けます。あまり多くのディスク・スペースを使用しないように、時々、そのファイルを削除することをお勧めします。また「**Server Properties - Channels**」ページを使用して、NAMED.RUN ファイルの最大サイズとバージョン数に対するプリファレンスを指定することができます。

DNS サーバー・インスタンスのデバッグ値を変更するには、以下のステップに従ってください。

1. **iSeries ナビゲーター**で、**使用する iSeries サーバー** —>「**ネットワーク**」—>「**サーバー**」—>「**DNS**」と展開します。
2. 右側のペインで**使用する DNS サーバー**を右クリックし、「**構成**」を選択します。
3. 「**DNS 構成**」ウィンドウで「DNS サーバー」を右クリックし、「**プロパティー**」を選択します。
4. 「**サーバー・プロパティー - 一般**」ページで、サーバー始動時のデバッグ・レベルを指定します。
5. サーバーが稼動中の場合は、サーバーをいったん停止して再始動してください。
   注 : デバッグ・レベルを変更しても、サーバーの稼動中はその変更が有効になりません。ここで

設定されたデバッグ・レベルはそのサーバーが次回、完全再始動される時に有効となります。サーバーが稼動中にデバッグ・レベルを変更する必要がある場合、拡張 DNS 機能を参照してください。

DNS に関するその他の情報

DNS および BIND 8 に関する多くの情報リソースがあります。以下のリストは、その中の使用可能なリソースのほんの一部を記述しています。

- DNS および BIND の第 3 版。Paul Albitz および Cricket Liu。出版元は、O'Reilly and Associates, Inc. Sebastopol, California, 1998 です。ISBN 番号 1-56592-512-2。これは DNS についての最も信頼のおける情報源です。
- Internet Software Consortium Web サイト は、BIND のニュース、リンク、およびその他のリソースについて記載しています。
- InterNIC サイトは、すべてのドメイン・ネーム登録機関のディレクトリーを保持しています。これは、Internet Corporation for Assigned Names and Numbers (ICANN) によって認可されています。
- DNS Resources Directory は、DNS 参照資料、および検討グループを含むその他の多くの DNS リソースへのリンクを提供します。また、DNS 関連 RFC のリストも提供します。

IBM マニュアルおよびレッドブック

- AS/400 TCP/IP Autoconfiguration: DNS and DHCP Support
  このレッドブックには、OS/400 に含まれるドメイン・ネーム・システム (DNS) サーバー・サポートおよび Dynamic Host Configuration Protocol (DHCP) サーバー・サポートを説明しています。このレッドブックの情報は、例を通して DNS および DHCP がサポートするインストール、調整、構成、およびトラブルシューティングを行うのに有効です。
  注 : このレッドブックは、V5R1 で使用可能な新しい BIND 8 機能を含んで改訂されていません。ただし、一般的な DNS の概念を参照するのによいマニュアルです。

Printed in Japan

日本アイ・ビー・エム株式会社
〒106-8711　東京都港区六本木3-2-12