System i

Система доменных имен

Версия 6, выпуск 1

System i

Система доменных имен

Версия 6, выпуск 1

Примечание

Перед началом работы с этой информацией и с описанным в ней продуктом ознакомьтесь со сведениями, приведенными в разделе “Примечания”, на стр. 43.

Это издание относится к версии 6, выпуску 1, модификации 0 IBM i5/OS (код продукта 5761-SS1), а также ко всем последующим выпускам и модификациям, если в новых изданиях не указано обратное. Данная версия работает не на всех моделях систем с сокращенным набором команд (RISC) и не работает на моделях с полным набором команд (CISC).

© Copyright International Business Machines Corporation 1998, 2008. Все права защищены.

Содержание

© Copyright IBM Corp. 1998, 2008

>Система имен доменов (DNS)

Система имен доменов (DNS) - это распределенная база данных, служащая для управления именами хостов и связанными с ними IP-адресами.

DNS позволяет применять для идентификации хостов символьные имена, например www.jkltoys.com, которые намного легче запомнить, чем IP-адреса, например, 192.168.12.88 в IPv4 или 2001:D88::1 в IPv6. Отдельный сервер отвечает за имена и IP-адреса хостов, относящиеся лишь к некоторой части области, однако за счет взаимодействия с другими серверами он может преобразовывать любые имена хостов в IP-адреса. За счет совместной работы серверов DNS компьютеры могут обмениваться данными по Internet.

В IBM i5/OS Version 6 Release 1 (V6R1) службы DNS основаны на общепринятой реализации DNS, известной как Служба доменных имен Internet, разработанная в университете Беркли (Berkeley Internet Name Domain - BIND) версии 9. Прежние выпуски служб DNS i5/OS были основаны на BIND версии 8.2.5. Для использования сервера DNS новой версии BIND 9 вам потребуется установить компоненты i5/OS 31 (DNS) и 33 (Portable Application Solutions Environment (PASE)) в вашей системе IBM System i. Начиная с i5/OS V6R1 версии BIND 4 и 8 заменены на BIND 9 из соображений защиты. Таким образом, обновление до BIND 9 является необходимым для вашего сервера DNS.

Новое в версии V6R1

В разделе предоставлена новая информация о Системе имен доменов (DNS) и информация о DNS, в которую внесены значительные изменения.

BIND 9

Berkeley Internet Name Domain (BIND) версии 9, представленный в этом выпуске, предоставляет ряд возможностей для повышения производительности сервера Системы имен доменов (DNS). Например, он поддерживает поиск адреса по имени и наоборот во всех определенных формах IPv6. Он использует оператор *view*, который позволяет одиночному экземпляру DNS по-разному отвечать на запрос в зависимости от того, откуда направлен запрос, например из Internet или внутренней сети. Кроме того, он использует файлы журнала для сохранения динамических обновлений для области.

Предыдущие версии BIND 4.9.3 и BIND 8.2.5 больше не поддерживаются и должны быть обновлены до BIND 9.

Новые команды настройки

Для упрощения работы с файлами конфигурации DNS были добавлены следующие команды настройки.

Создать конфигурацию RNDC (CRTRNDCCFG)
Команда настройки RNDC (CRTRNDCCFG) используется для создания файлов конфигурации RNDC. Благодаря ей, нет необходимости в написании файла rndc.conf и его соответствующих параметров и операторов для ключей в файле named.conf вручную.

Команда настройки DNS (CHKDNSCFG)
Команда настройки DNS (CHKDNSCFG) проверяет синтаксис файла конфигурации named.conf. Однако, она не обеспечивает семантическую проверку файла конфигурации.

Команда проверки областей DNS (CHKDNSZNE)
Команда проверки областей DNS (CHKDNSZNE) проверяет синтаксис и целостность файла информации об области. Ее можно использовать для проверки файлов информации об области перед его добавлением на сервер DNS.

© Copyright IBM Corp. 1998, 2008

Новые инструменты для работы с запросами и обновлениями

Указанные ниже инструменты для работы с запросами и обновлениями были добавлены для расширения возможностей по управлению сервером DNS.

Domain Information Groper (DIG)
Инструмент для работы с запросами DIG используется для получения информации о хостах, доменах DNS и других серверах DNS, основанной на ответе сервера DNS. Также его можно использовать перед настройкой системы для проверки правильности работы сервера DNS.

Запуск запроса HOST (HOST)
Команда Запуск запроса HOST (HOST) используется для просмотра DNS. Она преобразует имена доменов в IP-адреса (как IPv4, так и IPv6) и наоборот.

Команда динамического обновления (NSUPDATE)
Команда динамического обновления (NSUPDATE) передает на сервер DNS запросы на динамическое обновление DNS согласно запросу на комментарий (RFC) 2136. Это позволяет добавлять в область и удалять из нее записи о ресурсах во время работы сервера DNS. Поэтому нет необходимости в обновлении записей путем ручного редактирования файла области. Отдельный запрос на обновление может содержать запросы на добавление или удаление нескольких записей о ресурсах, но динамически добавляемые или удаляемые с помощью команды NSUPDATE записи о ресурсах должны находиться в одной и той же области.

Удаленное управление демоном имен (RNDC)
Команда Удаленное управление демоном имен (RNDC) позволяет системному администратору управлять работой сервера имен. Она прочитывает файл конфигурации *rndc.conf* для определения способа соединения с сервером имен, а также алгоритма и ключей, которые следует использовать. Если файл rndc.conf не найден, то по умолчанию файлом rndc-key._KID, который создается во время установки, автоматически предоставляет права доступа посредством циклического интерфейса.

Условное обозначение новой и измененной информации

Для упрощения поиска изменений в этом Information Center используются такие значки:

- Значок » отмечает начало новой или измененной информации.
- Значок « отмечает конец новой или измененной информации.

В документах PDF вы можете встретить пометки изменения (|) в левом поле напротив новой и измененной информации.

Ссылки, связанные с данной

“Новые возможности BIND 9” на стр. 8
Стандарт BIND 9 подобен стандарту BIND 8. Тем не менее, в нем предусмотрен ряд новых возможностей, позволяющих повысить производительность сервера Системы имен доменов (DNS), например представления.

Документ в формате PDF о Системе имен доменов

Можно просмотреть и распечатать файл PDF с данной информацией.

Для просмотра или загрузки этого документа в формате PDF выберите ссылку Domain Name System (около 625 Кб).

Сохранение файлов PDF

Для сохранения документа PDF на рабочей станции для дальнейшего просмотра или печати выполните следующие действия:

1. Щелкните правой кнопкой мыши на приведенной ссылке на документ PDF в окне браузера.

2. Щелкните на опции локального сохранения PDF.
3. Выберите каталог, в котором следует сохранить файл PDF.
4. Нажмите кнопку **Сохранить**.

Загрузка программы Adobe Reader

Для просмотра и печати документов в формате PDF необходима программа Adobe Reader. Бесплатную копию этой программы можно загрузить с Web-сайта Adobe по адресу Adobe Web site

(www.adobe.com/products/acrobat/readstep.html) .

Ссылки, связанные с данной

“Связанная информация по DNS” на стр. 42
Публикации IBM Redbooks, Web-сайты и другие разделы information center содержат информацию, которая связана с разделами о Системе имен доменов. Документы в формате PDF можно просмотреть или распечатать.

Краткая информация о DNS

Система имен доменов (DNS) - это система распределенных баз данных, предназначенная для управления именами хостов и связанными с ними IP-адресами. DNS позволяет применять для идентификации хостов символьные имена, например www.jkltoys.com, которые намного легче запомнить, чем IP-адреса, например, 192.168.12.88 в IPv4 или 2001:D88::1 в IPv6.

Отдельный сервер отвечает за имена и IP-адреса хостов, относящиеся лишь к некоторой части области, однако за счет взаимодействия с другими серверами он может преобразовывать любые имена хостов в IP-адреса. За счет совместной работы серверов DNS компьютеры могут обмениваться данными по Internet.

Вся информация DNS хранится в виде иерархии доменов. Каждый сервер отвечает за небольшую часть этой информации, например, за один субдомен. Часть домена, за которую отвечает сервер, называется областью. Сервер DNS, на котором хранится вся информация о хостах, относящихся к области, является ответственным за эту область. Ответственный сервер отвечает на запросы, связанные с хостами из его области, с помощью собственных записей о ресурсах. Процесс обработки запроса зависит от ряда факторов. Описание различных способов обработки запросов приведено в разделе Основные сведения о запросах DNS.

Основные сведения об областях

Вся информация Системы имен доменов (DNS) поделена на наборы данных, называемые *областями*. Каждый из этих наборов является специфическим типом области.

В области хранится часть информации об именах и IP-адресах, относящихся к домену DNS. Сервер, на котором хранится вся информация об области, является ответственным за область, называемую *родительской областью*. Иногда право на обработку запросов DNS, относящихся к какому-то субдомену, желательно передать другому серверу DNS, называемому *дочерней областью*. В этом случае в конфигурации сервера DNS, ответственного за домен, необходимо указать, что запросы, связанные с субдоменом, должны пересылаться другому серверу.

Довольно часто информация об области хранится не только на ответственном сервере DNS, но и на нескольких резервных серверах. Такие серверы называются вспомогательными. Они загружают информацию об области с ответственного сервера. Настройка вспомогательных серверов позволяет распределить нагрузку по нескольким серверам и получить резервную копию в случае сбоя основного сервера. Процедура загрузки информации об области на вспомогательный сервер называется передачей информации об области ответственности. После инициализации вспомогательный сервер загружает всю информацию об области с основного сервера. Впоследствии вспомогательный сервер загружает информацию об области с основного или другого вспомогательного сервера при изменении этой информации.

Типы областей DNS

Служба DNS системы i5/OS позволяет создавать области нескольких типов:

Основная область
Информация об этой области загружается из файла хоста. В основной области можно создать подобласть, или дочернюю область. Кроме того, эта область может содержать записи о ресурсах, например, записи с информацией о хосте, записи псевдонимов (CNAME), записи об адресе IPv4 (A), адресе IPv6 (AAAA) и записи с указателем для обратного преобразования (PTR).

Примечание: В другой документации по BIND основные области иногда называются *главными областями*.

Подобласть
Подобласть - это область внутри основной области. Подобласти позволяют разделить всю информацию об области на более мелкие части.

Дочерняя область
Дочерняя область - это подобласть, права на управление которой переданы одному или нескольким серверам имен.

Псевдоним (CNAME)
Псевдоним - это альтернативное имя домена основного сервера.

Хост Такой объект позволяет определить записи A и PTR, связанные с хостом. Для хоста могут быть определены дополнительные записи о ресурсах.

Вспомогательная область
Информация о вспомогательной области загружается с основного сервера или другого вспомогательного сервера. В ней хранится полная копия информации об области.

Примечание: В другой документации по BIND вспомогательные области иногда называются *подчиненными областями*.

Ограниченная область
Ограниченная область во многом аналогична вспомогательной области, однако в ней хранятся только копии записей NS из основной области.

Область пересылки
Областью пересылки называется область, все запросы к которой пересылаются другим серверам.

Понятия, связанные с данным

“Основные сведения о запросах DNS”
Для обработки запросов клиенты Системы имен доменов (DNS) используют серверы DNS. Запросы серверу могут отправляться как самими клиентами, так и другими работающими приложениями.

Задачи, связанные с данной

“Настройка областей сервера имен” на стр. 29
После настройки экземпляра сервера DNS необходимо настроить области сервера имен.

Ссылки, связанные с данной

“Пример: Сервер DNS для внутренней сети” на стр. 14
В этом примере описана простая подсеть, для которой настроен сервер DNS.

“Записи о ресурсах DNS” на стр. 10
В записях о ресурсах хранится информация об именах хостов и IP-адресах. Для просмотра записей о ресурсах, поддерживаемых операционной системой i5/OS, можно воспользоваться Таблицей записей о ресурсах.

Основные сведения о запросах DNS

Для обработки запросов клиенты Системы имен доменов (DNS) используют серверы DNS. Запросы серверу могут отправляться как самими клиентами, так и другими работающими приложениями.

Такой запрос содержит полное имя хоста (FQDN), тип запроса, например, тип записи, которая необходима клиенту, и класс имени домена (большинство имен относятся к классу Internet - IN). На приведенном ниже рисунке показан пример сети, описанный в разделе Сервер DNS, подключенный к Internet.

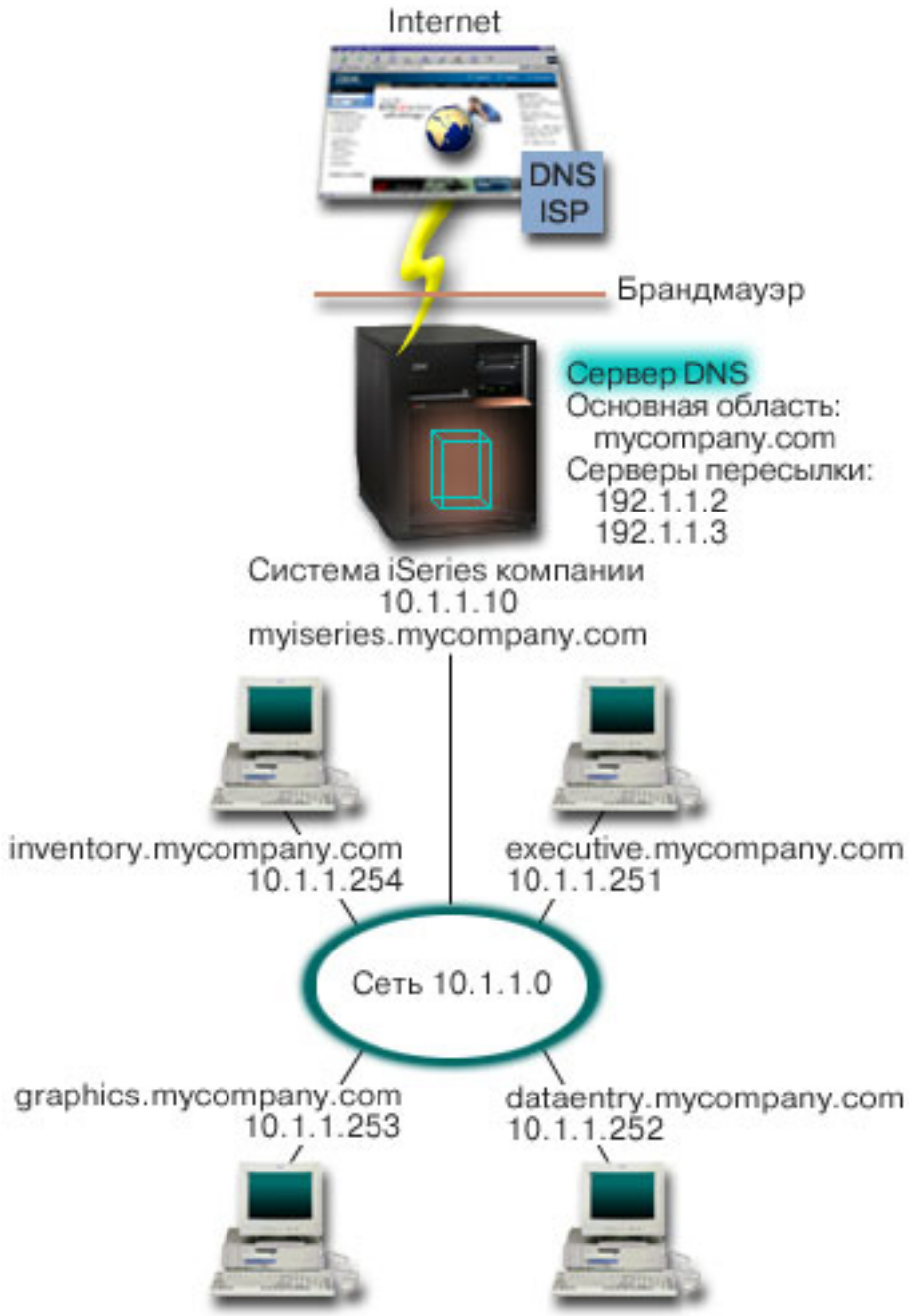

Рисунок 1. Сервер DNS, подключенный к Internet

Предположим, что хост *dataentry* отправляет серверу DNS запрос на получение информации о хосте graphics.mycompany.com. Сервер DNS просмотрит собственную информацию об области и отправит клиенту ответ с информацией о том, что IP-адрес хоста равен 10.1.1.253.

Теперь предположим, что хост *dataentry* отправил запрос на получение IP-адреса хоста www.jkl.com. Сведения об этом хосте отсутствуют в информации об области сервера DNS. Можно использовать один из

двух способов настройки: *рекурсивный* или *циклический*. Если на сервере DNS настроен *рекурсивный* способ обработки запросов, то сервер обратится с запросом на преобразование имени к другим серверам DNS от имени клиента, отправившего исходный запрос, а затем перешлет клиенту полученный ответ. Кроме того, сервер, который отправил запрос, сохраняет ответ в кэше, чтобы можно было использовать этот ответ в следующий раз при получении данного запроса. Если на сервере DNS настроен *циклический* способ, то клиент может попытаться самостоятельно обратиться к другим серверам DNS для преобразования имени хоста. При таком способе обработки запроса клиент отправляет запросы серверам из имеющегося списка, а затем - дополнительным серверам, которым был переадресован запрос исходными серверами.

Ссылки, связанные с данной

“Основные сведения об областях” на стр. 3
Вся информация Системы имен доменов (DNS) поделена на наборы данных, называемые *областями*. Каждый из этих наборов является специфическим типом области.

“Пример: Сервер DNS, подключенный к Internet” на стр. 16
В этом примере описана простая подсеть, в которой настроен сервер DNS, подключенный к Internet.

Настройка домена DNS

Для настройки Системы имен доменов (DNS) требуется зарегистрировать имя домена, чтобы никто кроме вас не смог его использовать.

Вы можете настроить сервер DNS, который будет обслуживать запросы на преобразование имен и адресов хостов во внутренней сети. Кроме того, если сервер будет подключен к Internet, то он сможет обрабатывать запросы, поступающие от внешних хостов. Для настройки домена в Internet необходимо зарегистрировать имя домена.

Для обработки внутренних запросов не требуется регистрировать имя домена. Однако вы можете зарегистрировать имя домена для того, чтобы никто не мог зарегистрировать домен Internet с таким именем. Это имеет смысл сделать в том случае, если в дальнейшем вы планируете использовать этот домен во внешней сети.

Для регистрации домена можно обратиться в специальную службу регистрации имен доменов, либо к провайдеру Internet (ISP), оказывающему такие услуги. Некоторые ISP могут зарегистрировать домен от имени клиента. Список служб регистрации имен доменов, уполномоченных организацией ICANN, можно найти на Web-сайте Internet Network Information Center (InterNIC).

Ссылки, связанные с данной

“Пример: Сервер DNS, подключенный к Internet” на стр. 16
В этом примере описана простая подсеть, в которой настроен сервер DNS, подключенный к Internet.

Информация, связанная с данной

Internet Network Information Center (InterNIC)

Динамическое обновление данных DNS

i5/OS Система имен доменов (DNS) с применением стандарта BIND 9 поддерживает динамическое обновление. Запросы на динамическое обновление отправляются некоторыми внешними службами, в частности, службой Протокола динамической настройки хостов (DHCP). Для динамического обновления можно использовать также и инструменты клиента, например программу динамического обновления (NSUPDATE).

DHCP - это стандартный протокол TCP/IP, который позволяет настроить центральный сервер, предоставляющий IP-адреса и другую информацию о конфигурации устройствам сети. В ответ на запросы клиентов сервер DHCP отправляет динамически созданное описание конфигурации. Вы можете определить параметры конфигурации хостов на центральном сервере DHCP, который будет автоматически сообщать эти параметры хостам. Этот протокол обычно применяется для выделения временных IP-адресов клиентам, когда число клиентов в сети превосходит число доступных IP-адресов.

Раньше вся информация DNS хранилась в статической базе данных. Все записи о ресурсах DNS вручную создавались и обслуживались администратором. Но серверы DNS, поддерживающие BIND 8 и выше можно настроить на прием запросов на динамическое обновление информации об области из других источников.

В конфигурации сервера DHCP можно указать, что при выделении адреса хосту должен отправляться запрос на обновление информации DNS. В быстро растущих или постоянно изменяющихся сетях TCP/IP, а также в сетях с часто изменяющейся топологией такая функция позволяет значительно сэкономить время администратора сервера DNS. Информация о том, что клиент получил от сервера DHCP некоторый IP-адрес, немедленно отправляется серверу DNS. За счет этого сервер DNS может обрабатывать запросы на получение IP-адресов хостов даже тогда, когда эти адреса часто меняются.

Сервер DHCP может обновлять от имени клиента записи об адресе (A для IPv4 или AAAA для IPv6), записи обратного преобразования (PTR) или оба типа записей. В записи об адресе (A или AAAA) хранится IP-адрес, связанный с именем хоста. В записи PTR хранится имя хоста, связанное с IP-адресом. При изменении адреса клиента сервер DHCP может автоматически отправить запрос на обновление информации DNS, для того чтобы другие хосты сети могли узнать новый IP-адрес клиента от сервера DNS. Для каждой обновленной записи создана текстовая запись (TXT), содержащая информацию о том, от кого был получен запрос на обновление (в данном случае - от DHCP).

Примечание: Если сервер DHCP будет обновлять только записи PTR, клиентам должно быть разрешено обновлять информацию на сервере DNS. В этом случае каждый клиент самостоятельно обновит свою запись типа A, если клиент использует адрес IPv4, или AAAA, если клиент использует адрес IPv6. Обратите внимание, что не все клиенты DHCP поддерживают обновление собственной записи типа A или AAAA. Перед настройкой такого способа динамического обновления ознакомьтесь с документацией по операционной системе, установленной на компьютерах-клиентах.

Для защиты динамически обновляемых областей создается список служб, которым предоставлены права на отправку запросов на обновление. Такие права могут быть предоставлены отдельным IP-адресам, целым подсетям, а также пакетам, подписанным с помощью общего секретного ключа (который называется *Подпись транзакции*, или TSIG). Перед обновлением записей о ресурсах сервер DNS проверяет, что пакет с запросом на обновление отправлен службой с соответствующими правами доступа.

Функция динамического обновления может применяться в том случае, когда серверы DNS и DHCP расположены в одной системе System i, в разных системах System i, а также между системами System i и другими системами, которые поддерживают динамическое обновление.

Примечание: Для отправки запросов на динамическое обновление информации DNS в системе должен быть доступен API QTOBUPDT. Этот API автоматически устанавливается вместе с компонентом 31 (DNS) i5/OS. Тем не менее, для обновления системы System i в BIND 9 рекомендуется использовать команду NSUPDATE.

Понятия, связанные с данным

Dynamic Host Configuration Protocol

Задачи, связанные с данной

“Настройка функции динамического обновления на сервере DNS” на стр. 30
Серверы DNS, поддерживающие BIND 9, могут принимать запросы на динамическое обновление информации об области от различных служб. В этом разделе приведены инструкции по настройке функции динамического обновления на сервере DNS.

Настройка функции динамического обновления DNS на сервере DHCP

Ссылки, связанные с данной

“Пример: серверы DNS и DHCP в одной и той же системе System i” на стр. 18
В этом примере описана работа с серверами DNS и DHCP, расположенные в одной и той же системе System i.

“Записи о ресурсах DNS” на стр. 10
В записях о ресурсах хранится информация об именах хостов и IP-адресах. Для просмотра записей о ресурсах, поддерживаемых операционной системой i5/OS, можно воспользоваться Таблицей записей о ресурсах.

QTOBUPT

“Новые возможности BIND 9”
Стандарт BIND 9 подобен стандарту BIND 8. Тем не менее, в нем предусмотрен ряд новых возможностей, позволяющих повысить производительность сервера Системы имен доменов (DNS), например представления.

Новые возможности BIND 9

Стандарт BIND 9 подобен стандарту BIND 8. Тем не менее, в нем предусмотрен ряд новых возможностей, позволяющих повысить производительность сервера Системы имен доменов (DNS), например представления.

Представления на одиночном сервере DNS i5/OS

Оператор *view* позволяет одиночному экземпляру DNS по-разному отвечать на запрос в зависимости от того, откуда направлен запрос, например из Internet или внутренней сети.

Одно из практических применений представлений - разделение настроек DNS без использования нескольких серверов DNS. Например, на одиночном сервере DNS можно определить одно представление для ответов на запросы из внутренней сети, а другое представление для ответов на запросы из внешней сети.

Новые команды клиента

Указанные ниже команды клиента расширяют возможности по управлению сервером DNS:

Программа динамического обновления (NSUPDATE)
Команда динамического обновления (NSUPDATE) передает на сервер DNS запросы на динамическое обновление DNS согласно запросу на комментарий (RFC) 2136. Это позволяет добавлять в область и удалять из нее записи о ресурсах во время работы сервера DNS. Поэтому нет необходимости в обновлении записей путем ручного редактирования файла области. Отдельный запрос на обновление может содержать запросы на добавление или удаление нескольких записей о ресурсах, но динамически добавляемые или удаляемые с помощью команды NSUPDATE записи о ресурсах должны находиться в одной и той же области.

Примечание: Не изменяйте вручную те области, которые находятся под динамическим управлением команды NSUPDATE или сервера DHCP. Изменения, которые вносятся вручную, могут конфликтовать с динамическими обновлениями, что приведет к потере данных.

Запуск запроса DIG (DIG)
Domain Information Groper (DIG) является более мощным инструментом по работе с запросами, чем команда Просмотр информации сервера имен (NSLOOKUP), которую можно использовать для получения информации с сервера DNS или тестирования ответов сервера DNS. Команда NSLOOKUP устарела и предусмотрена только для совместимости с более ранними версиями. Перед настройкой системы можно использовать DIG для проверки правильности работы сервера DNS. Также с помощью DIG можно получать информацию о хостах, доменах DNS и других серверах DNS.

Команду Запуск запроса DIG (STRDIGQRY) или ее псевдоним DIG можно использовать для запуска инструмента Domain Information Groper.

Запуск запроса HOST (HOST)
Команда Запуск запроса HOST (HOST) используется для просмотра DNS. Ее можно использовать для преобразования имен доменов в IP-адреса (как IPv4, так и IPv6) и наоборот.

Удаленное управление демоном имен (RNDC)

Команда Удаленное управление демоном имен (RNDC) является мощным инструментом, позволяющим системному администратору управлять работой сервера имен. Она прочитывает файл конфигурации rndc.conf для определения способа соединения с сервером имен, а также алгоритма и ключей, которые следует использовать. Если файл rndc.conf не найден, то по умолчанию файлом rndc-key._KID, который создается во время установки, автоматически предоставляет права доступа посредством циклического интерфейса.

Поддержка IPv6

BIND 9 поддерживает поиск адреса по имени и наоборот во всех определенных формах IPv6. Для прямого преобразования BIND 9 поддерживает записи AAAA и A6, но записи A6 являются устаревшими. Для обратного преобразования IPv6 он поддерживает традиционный формат ”полубайтов”, используемый в домене ip6.arpa, а также в устаревшем домене ip6.int.

Файлы журналов

Файлы журналов предназначены для хранения динамических обновлений области. Они создаются автоматически при получении первого динамического обновления от клиента и не удаляются. Они являются двоичными, и их не следует редактировать.

Благодаря файлам журналов при перезапуске сервера после завершения работы или сбоя системы этот сервер воспроизводит действия, зарегистрированные в файле журнала, для применения всех обновлений области, которые происходили после создания последнего дампа области. Файлы журналов предназначены также для хранения обновлений с использованием метода передачи измененной информации об области (IXFR).

DNS для системы i5/OS был переработан для использования BIND 9. Для работы DNS BIND 9 в вашей системе требуется наличие определенного программного обеспечения.

Понятия, связанные с данным

“Требования DNS” на стр. 26
В этом разделе приведен список программного обеспечения, которое требуется для работы DNS в системе System i.

“Динамическое обновление данных DNS” на стр. 6
i5/OS Система имен доменов (DNS) с применением стандарта BIND 9 поддерживает динамическое обновление. Запросы на динамическое обновление отправляются некоторыми внешними службами, в частности, службой Протокола динамической настройки хостов (DHCP). Для динамического обновления можно использовать также и инструменты клиента, например программу динамического обновления (NSUPDATE).

“Новое в версии V6R1” на стр. 1
В разделе предоставлена новая информация о Системе имен доменов (DNS) и информация о DNS, в которую внесены значительные изменения.

Ссылки, связанные с данной

“Пример: Разделение областей ответственности DNS в сети с брандмауэром путем настройки двух серверов DNS в одной системе System i” на стр. 20
В этом примере описана настройка сервера DNS в сети с брандмауэром, который защищает данные внутренних хостов от внешних пользователей, не ограничивая доступ внутренних пользователей к Internet. Такая конфигурация защищает данные путем настройки двух серверов DNS в одной системе System i.

“Планирование мер защиты” на стр. 25
В службе DNS предусмотрен ряд средств защиты, позволяющих ограничить доступ внешних пользователей к серверу.

Записи о ресурсах DNS

В записях о ресурсах хранится информация об именах хостов и IP-адресах. Для просмотра записей о ресурсах, поддерживаемых операционной системой i5/OS, можно воспользоваться Таблицей записей о ресурсах.

База данных об области DNS содержит набор записей о ресурсах. Запись о ресурсе содержит информацию о некотором объекте. Например, запись об адресе (A) содержит IP-адрес, связанный с именем хоста, а запись обратного преобразования (PTR) содержит имя хоста, связанное с IP-адресом. Эти записи применяются сервером для обработки запросов на получение информации о хостах, относящихся к его области. Для того чтобы ознакомиться с описаниями различных записей о ресурсах DNS, выберите тип записи в приведенной ниже таблице.

Примечание: Записи в Таблице записей о ресурсах могут добавляться или удаляться согласно изменениям в документе BIND. Кроме того, эта таблица не содержит полный список всех записей о ресурсах, перечисленных в BIND.

Таблица 1. Таблица записей о ресурсах

Запись	Аббревиатура	Описание
Записи преобразования адресов	A	Запись A задает IP-адрес этого хоста. С помощью записей A выполняется запрос на преобразование имени домена в IP-адрес. Этот тип записей определен в RFC 1035.
Записи базы данных файловой системы Andrew	AFSDB	Запись AFSDB содержит адрес AFS или DCE объекта. Записи AFSDB, как и записи A, применяются для преобразования имени домена в адрес AFSDB; либо для преобразования имени домена кластера в адрес сервера идентифицируемого имени кластера. Этот тип записей определен в RFC 1183.
Записи полных имен	CNAME	Запись CNAME содержит фактическое имя домена данного объекта. Если DNS при обращении к псевдониму обнаруживает запись CNAME, содержащую полное имя, DNS затем запрашивает полное имя домена. Этот тип записей определен в RFC 1035.
Записи информации о хосте	HINFO	Запись HINFO содержит общую информацию о хосте. Стандартные имена процессоров и операционных систем определены в RFC 1700. Использование стандартных номеров не является обязательным. Этот тип записей определен в RFC 1035.
Записи Цифровой сети с комплексными услугами	ISDN	Запись ISDN содержит адрес этого объекта. Эта запись предназначена для преобразования имен хостов в адреса ISDN. Они используются только в сетях ISDN. Этот тип записей определен в RFC 1183.

Таблица 1. Таблица записей о ресурсах (продолжение)

Запись	Аббревиатура	Описание
Записи IP-адресов версии 6	AAAA	Запись AAAA содержит 128-разрядный адрес хоста для IPv6. Записи AAAA, которые подобны записям A, используются для преобразования запросов для адреса IPv6 определенного имени домена. Этот тип записи определен в RFC 1886.
Записи расположения	LOC	Запись LOC содержит информацию о физическом расположении элементов сети. Такие записи применяются в приложениях для оценки эффективности работы сети или построения схемы физического расположения узлов сети. Этот тип записей определен в RFC 1876.
Записи Системы обмена почтой	MX	Записи MX содержат определение хоста системы обмена почтой для почтовых сообщений, отправляемых в этот домен. С помощью записей этого типа и значений параметров конфигурации хостов системы обмена почтой в SMTP (Простой протокол передачи почты) определяются адреса хостов, обрабатывающих и перенаправляющих почту для этого домена. Каждому хосту системы обмена почтой должна соответствовать запись адреса хоста (A) в существующей области. Этот тип записей определен в RFC 1035.
Записи почтовой группы	MG	Записи MG указывают имя домена почтовой группы. Этот тип записей определен в RFC 1035.
Записи почтового ящика	MB	Запись MB содержит имя домена хоста, на котором расположен почтовый ящик данного объекта. Почтовые сообщения, отправляемые в этот домен, перенаправляются на хост, который указан в записи MB. Этот тип записей определен в RFC 1035.
Записи информации о почтовом ящике	MINFO	Запись MINFO указывает почтовый ящик, в который должны направляться сообщения об ошибках для данного объекта. Записи MINFO чаще применяются для списков рассылки, чем для отдельных почтовых ящиков. Этот тип записей определен в RFC 1035.

Таблица 1. Таблица записей о ресурсах (продолжение)

Запись	Аббревиатура	Описание
Записи нового имени почтового ящика	MR	Запись MR указывает новое имя домена почтового ящика. Запись MR позволяет пользователям, сменившим почтовый ящик, перенаправлять входящие почтовые сообщения. Этот тип записей определен в RFC 1035.
Записи сервера имен	NS	Запись NS указывает ответственный сервер для данного хоста. Этот тип записей определен в RFC 1035.
Запись протокола доступа к сетевым службам	NSAP	Запись NSAP содержит адрес ресурса NSAP. Записи NSAP предназначены для преобразования имен доменов в адреса NSAP. Этот тип записей определен в RFC 1706.
Записи общих ключей	KEY	Запись KEY содержит общий ключ, связанный с именем DNS. Ключ может относиться к области, пользователю или хосту. Этот тип записей определен в RFC 2065.
Записи ответственных работников	RP	Запись RP содержит электронный адрес и описание лица, ответственного за область или хост. Этот тип записей определен в RFC 1183.
Записи указателей обратного преобразования	PTR	Запись PTR содержит имя домена хоста, для которого необходимо определить запись PTR. Запись PTR позволяет преобразовать IP-адрес в имя хоста. Этот тип записей определен в RFC 1035.
Записи маршрутизации	RT	Запись RT указывает имя домена хоста, который может перенаправлять IP-пакеты для данного хоста. Этот тип записей определен в RFC 1183.
Записи о службах	SRV	Запись SRV задает хосты, которые поддерживают службы, определенные записью. Этот тип записи определен в RFC 2782.
Запись начала области ответственности	SOA	Запись SOA означает, что данный сервер является ответственным за область. Ответственный сервер - это лучший источник для сбора данных внутри области. Запись SOA содержит общую информацию об области и правила перезагрузки для резервных серверов. Для каждой области создается только одна запись SOA. Этот тип записей определен в RFC 1035.

Таблица 1. Таблица записей о ресурсах (продолжение)

Запись	Аббревиатура	Описание
Текстовые записи	TXT	Запись TXT состоит из нескольких строк текста, связанных с именем домена, каждая длиной до 255 символов. Записи TXT можно использовать наряду с записями ответственных работников (RP) для хранения информации о лице, ответственном за область. Этот тип записей определен в RFC 1035. Записи TXT используются DHCP i5/OS для динамического обновления. Сервер DHCP создает запись TXT для каждого внесенного им обновления записей A и PTR. Записи сервера DHCP начинаются с символов AS400DHCP.
Записи стандартных служб	WKS	Записи WKS указывают стандартные службы, поддерживаемые объектом. Чаще всего записи WKS содержат информацию о поддержке протоколов TCP и UDP для данного адреса. Этот тип записей определен в RFC 1035.
Записи преобразования адресов X.400	PX	Запись PX содержит указатель на информацию о преобразовании X.400/RFC 822. Этот тип записей определен в RFC 1664.
Записи преобразования адресов X25	X25	Запись X25 содержит адрес ресурса X25. Записи X25 предназначены для преобразования имен хостов в адреса PSDN. Они используются только в сетях X25. Этот тип записей определен в RFC 1183.

Понятия, связанные с данным

"Записи о почтовом шлюзе и записи MX"
DNS поддерживает маршрутизацию почты с помощью почтовых записей MX.

Ссылки, связанные с данной

"Пример: Сервер DNS для внутренней сети" на стр. 14
В этом примере описана простая подсеть, для которой настроен сервер DNS.

"Основные сведения об областях" на стр. 3
Вся информация Системы имен доменов (DNS) поделена на наборы данных, называемые *областями*. Каждый из этих наборов является специфическим типом области.

Записи о почтовом шлюзе и записи MX

DNS поддерживает маршрутизацию почты с помощью почтовых записей MX.

Записи о почтовом шлюзе и записи MX применяются программой пересылки почты, например, SMTP. Таблица записей о ресурсах DNS содержит типы почтовых записей, поддерживаемых на сервере DNS i5/OS.

Для организации обмена почтой на сервере DNS предусмотрены записи Системы обмена почтой. В сети с DNS приложение SMTP доставляет почту, адресованную хосту TEST.IBM.COM, не просто открывая соединение TCP с TEST.IBM.COM. Сначала SMTP отправляет на сервер DNS запрос о том, какие серверы хоста можно использовать для доставки почтового сообщения.

Доставка почты на определенный адрес

Серверы DNS работают с записями ресурсов, называемыми записями *Системы обмена почтой* (MX). В этих записях имени домена или хоста ставятся в соответствие имя хоста и коэффициент предпочтения. Обычно в записях типа MX указывается хост, который будет обрабатывать почту для некоторого хоста, а также другой, вспомогательный хост для случая, если первый хост окажется недоступен. Таким образом, записи типа MX позволяют направлять почту, адресованную одному хосту, на другой хост.

Для одного домена или имени хоста могут существовать несколько записей типа MX. Порядок, в котором они выбираются, определяется коэффициентом предпочтения (или приоритетом) каждой записи. Наименьший коэффициент обозначает наиболее предпочтительный вариант - запись, которая будет выбрана первой. Если наиболее предпочтительный хост недоступен, приложение, отправляющее почту, попытается подключиться к следующему по приоритету хосту. Приоритет задается администратором домена или создателем записи типа MX.

Если имя, указанное в запросе, находится в области ответственности сервера DNS, но для него нет ни одной записи типа MX, то сервер может вернуть пустой список записей типа MX. В этом случае приложение, отправляющее почту, попытается установить прямое соединение с целевым хостом.

Примечание: В записях MX не рекомендуется указывать имена доменов с символами подстановки (например, `*.mycompany.com`).

Пример записи типа MX для хоста

В следующем примере для доставки почты хосту fsc5.test.ibm.com приложение сначала (согласно установленным приоритетам) попытается установить прямое соединение с этим хостом. Если хост окажется недоступен, то почта должна быть доставлена на psfred.test.ibm.com или (если и он будет недоступен) - на mvs.test.ibm.com. Записи типа MX будут выглядеть следующим образом:

```
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
```

Ссылки, связанные с данной

“Записи о ресурсах DNS” на стр. 10
В записях о ресурсах хранится информация об именах хостов и IP-адресах. Для просмотра записей о ресурсах, поддерживаемых операционной системой i5/OS, можно воспользоваться Таблицей записей о ресурсах.

Примеры: Система имен доменов

Ознакомьтесь с примерами, чтобы понять, как работает служба DNS вашей сети.

DNS - это система распределенных баз данных, предназначенная для управления именами хостов и связанными с ними IP-адресами. Ниже приведены примеры, которые позволяют понять принципы работы сервера DNS и функции, которые он выполняет в сети. В этих примерах описана конфигурация сервера и его назначение. Кроме того, в них приведены ссылки на определения некоторых понятий, которые позволят вам лучше понять приведенные рисунки.

Пример: Сервер DNS для внутренней сети

В этом примере описана простая подсеть, для которой настроен сервер DNS.

На приведенном ниже рисунке изображен сервер DNS, настроенный в системе System i для внутренней сети. Этот экземпляр сервера получает запросы через все интерфейсы IP. Он играет роль основного сервера имен для области mycompany.com.

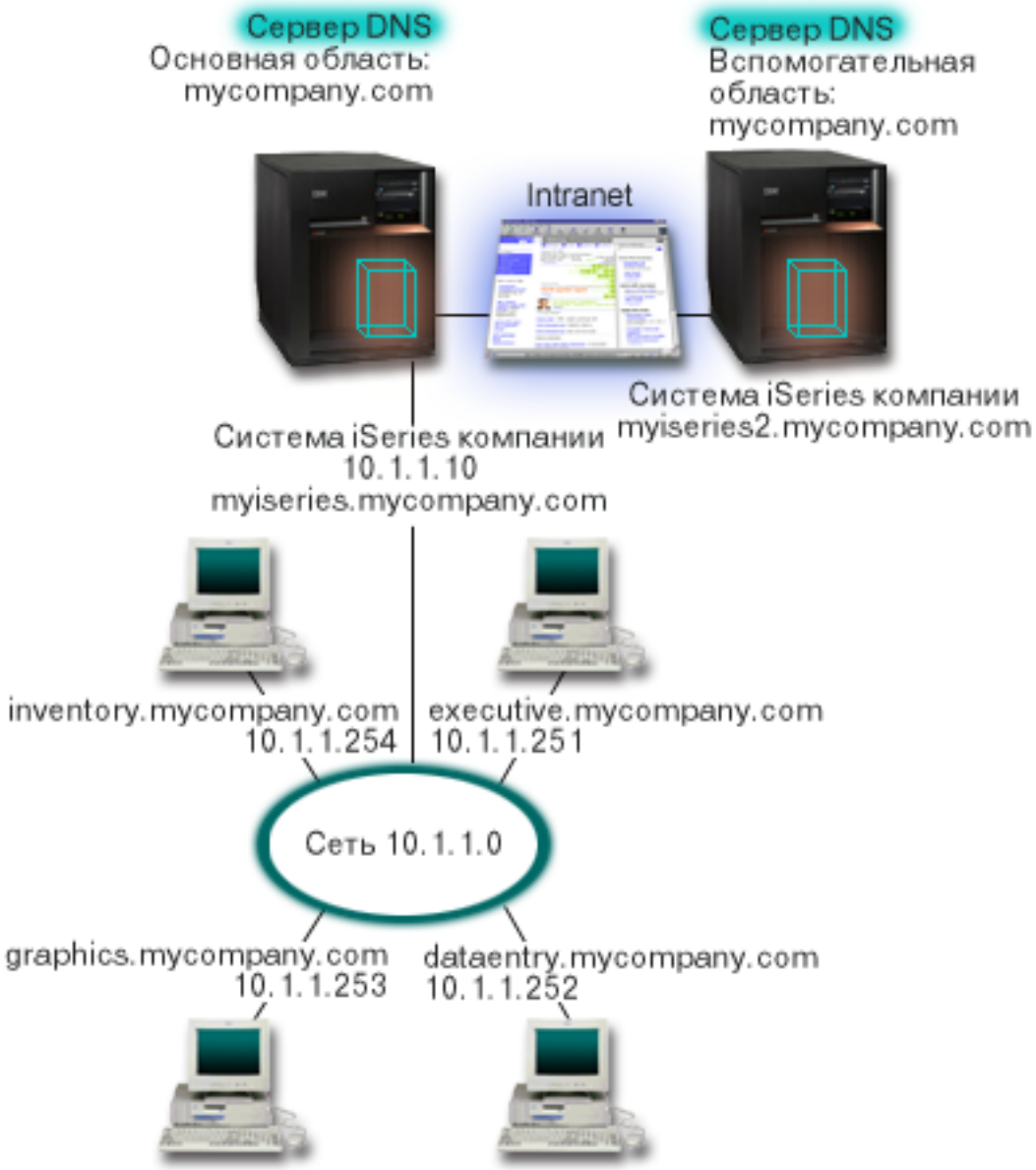

Рисунок 2. Отдельный сервер DNS для внутренней сети.

Каждому хосту области присвоены IP-адрес и имя хоста. Администратор должен вручную создать записи о ресурсах для хостов области DNS. Записи об адресе (A для IPv4 или AAAA для IPv6) служат для преобразования имени хоста в его IP-адрес. Это позволяет другим хостам сети отправлять серверу DNS запросы на получение IP-адреса, связанного с указанным именем хоста. Записи обратного преобразования (PTR) служат для преобразования IP-адреса компьютера в имя хоста. Это позволяет другим хостам сети отправлять серверу DNS запросы на получение имени хоста, связанного с указанным IP-адресом.

Помимо записей типа A, AAAA и PTR сервер DNS поддерживает многие другие записи о ресурсах, запросы на получение которых могут отправлять клиенты. Набор создаваемых записей зависит от того, какие приложения, применяющие TCP/IP, используются пользователями внутренней сети. Например, если в сети применяется программа электронной почты, то на сервере потребуется создать записи системы обмена почтой (MX), для того чтобы служба SMTP могла получать от сервера DNS информацию о том, в каких системах установлены почтовые серверы.

Если бы данная сеть входила в более крупную корпоративную сеть, то потребовалось бы определить внутренние корневые серверы.

Вспомогательные серверы

Вспомогательные серверы загружают информацию об области с сервера, ответственного за эту область. Процедура загрузки информации об области на вспомогательный сервер называется передачей информации об области ответственности. При запуске вспомогательный сервер загружает с основного сервера имен всю информацию о домене. Затем вспомогательный сервер имен загружает обновленную информацию с основного сервера, когда он получает соответствующее уведомление от основного сервера (если включена функция NOTIFY), либо когда он обращается к основному серверу и обнаруживает, что информация была изменена. На приведенном выше рисунке сервер mysystemi подключен к внутренней сети. Другая система, mysystemi2, играет роль вспомогательного сервера DNS для области mycompany.com. Вспомогательный сервер уменьшает нагрузку на основной сервер и заменяет его в случае сбоя. Для каждой области рекомендуется создавать по крайней мере по одному вспомогательному серверу.

Ссылки, связанные с данной

“Записи о ресурсах DNS” на стр. 10
В записях о ресурсах хранится информация об именах хостов и IP-адресах. Для просмотра записей о ресурсах, поддерживаемых операционной системой i5/OS, можно воспользоваться Таблицей записей о ресурсах.

“Основные сведения об областях” на стр. 3
Вся информация Системы имен доменов (DNS) поделена на наборы данных, называемые *областями*. Каждый из этих наборов является специфическим типом области.

“Пример: Сервер DNS, подключенный к Internet”
В этом примере описана простая подсеть, в которой настроен сервер DNS, подключенный к Internet.

Пример: Сервер DNS, подключенный к Internet

В этом примере описана простая подсеть, в которой настроен сервер DNS, подключенный к Internet.

На приведенном ниже рисунке приведена та же схема сети, что и в примере Сервер DNS для внутренней сети, однако теперь предполагается, что эта сеть подключена к Internet. Рассмотрим случай, когда пользователям внутренней сети разрешено работать в Internet, однако брандмауэр блокирует все данные, поступающие из Internet во внутреннюю сеть.

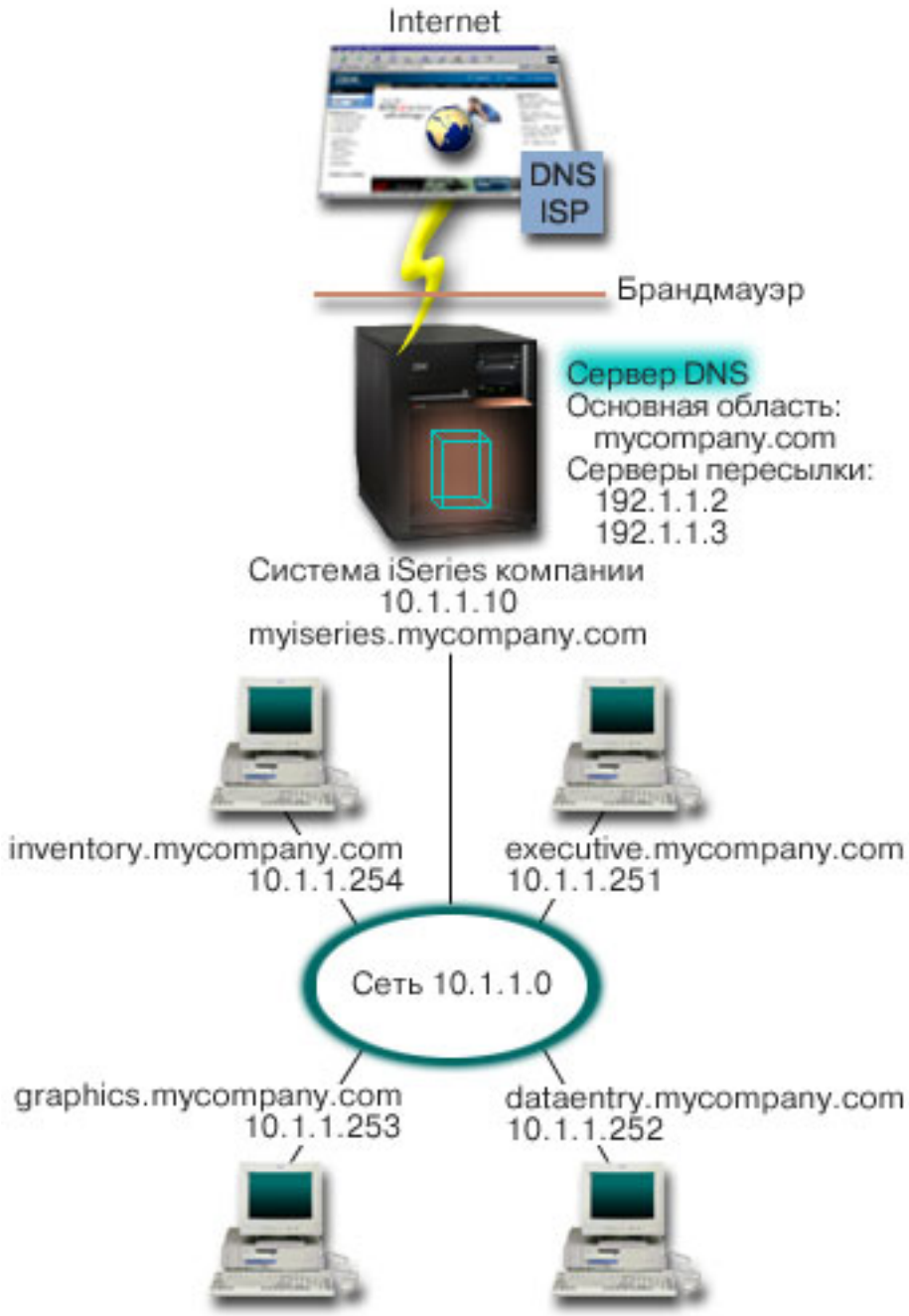

Рисунок 3. Сервер DNS, подключенный к Internet

Для того чтобы у сервера появилась возможность преобразовывать адреса хостов Internet, выполните по крайней мере одно из следующих действий:

- Определите корневые серверы Internet

  Список корневых серверов Internet, применяемых по умолчанию, можно загрузить автоматически, однако вам может потребоваться обновить этот список. Эти серверы позволяют отвечать на запросы, связанные с адресами, не входящими в локальную область. Инструкции по получению текущего списка корневых серверов Internet приведены в разделе Просмотр данных внешней Системы имен доменов.
- Разрешите пересылку запросов

Вы можете настроить сервер таким образом, чтобы все запросы, не относящиеся к области mycompany.com, пересылались внешним серверам DNS, например, серверам DNS вашего провайдера Internet (ISP). Если поиск необходимых записей должен выполняться как на корневых серверах, так и на серверах пересылки, укажите в параметре `forward` значение **first**. В этом случае сервер вначале обратится к серверам пересылки, а затем, если от них не будет получен ответ, к корневым серверам.

Помимо этого, может потребоваться внести следующие изменения в конфигурацию:

- Присвойте свободные IP-адреса

  В приведенном выше примере указаны адреса 10.x.x.x. Однако эти адреса могут применяться только во внутренней сети. Они приведены только в качестве примера. Адреса в вашей сети назначаются ISP и зависят от конфигурации сети.
- Зарегистрируйте имя домена

  Если вы хотите, чтобы ваш домен был доступен в Internet, зарегистрируйте имя домена.
- Настройте брандмауэр

  Не рекомендуется напрямую подключать сервер DNS к Internet. Вам следует настроить брандмауэр или принять какие-либо другие меры по защите системы System i.

Понятия, связанные с данным

“Настройка домена DNS” на стр. 6
Для настройки Системы имен доменов (DNS) требуется зарегистрировать имя домена, чтобы никто кроме вас не смог его использовать.

Защита системы System i при работе с Internet

“Основные сведения о запросах DNS” на стр. 4
Для обработки запросов клиенты Системы имен доменов (DNS) используют серверы DNS. Запросы серверу могут отправляться как самими клиентами, так и другими работающими приложениями.

Ссылки, связанные с данной

“Пример: Сервер DNS для внутренней сети” на стр. 14
В этом примере описана простая подсеть, для которой настроен сервер DNS.

Пример: серверы DNS и DHCP в одной и той же системе System i

В этом примере описана работа с серверами DNS и DHCP, расположенные в одной и той же системе System i.

Такая конфигурация позволяет серверу DHCP автоматически обновлять информацию об области на сервере DNS каждый раз, когда хосту присваивается новый IP-адрес.

На приведенном ниже рисунке показана схема небольшой подсети, к которой подключена одна система System i, выполняющая роль сервера DNS и DHCP. Предположим, что в этой подсети программы учета и приложения для администрирования, играющие роль клиентов, создают документы, которые содержат графические данные и хранятся на сервере графических файлов. Для получения данных с сервера графических файлов они подключают сетевой диск, указывая имя хоста этого сервера.

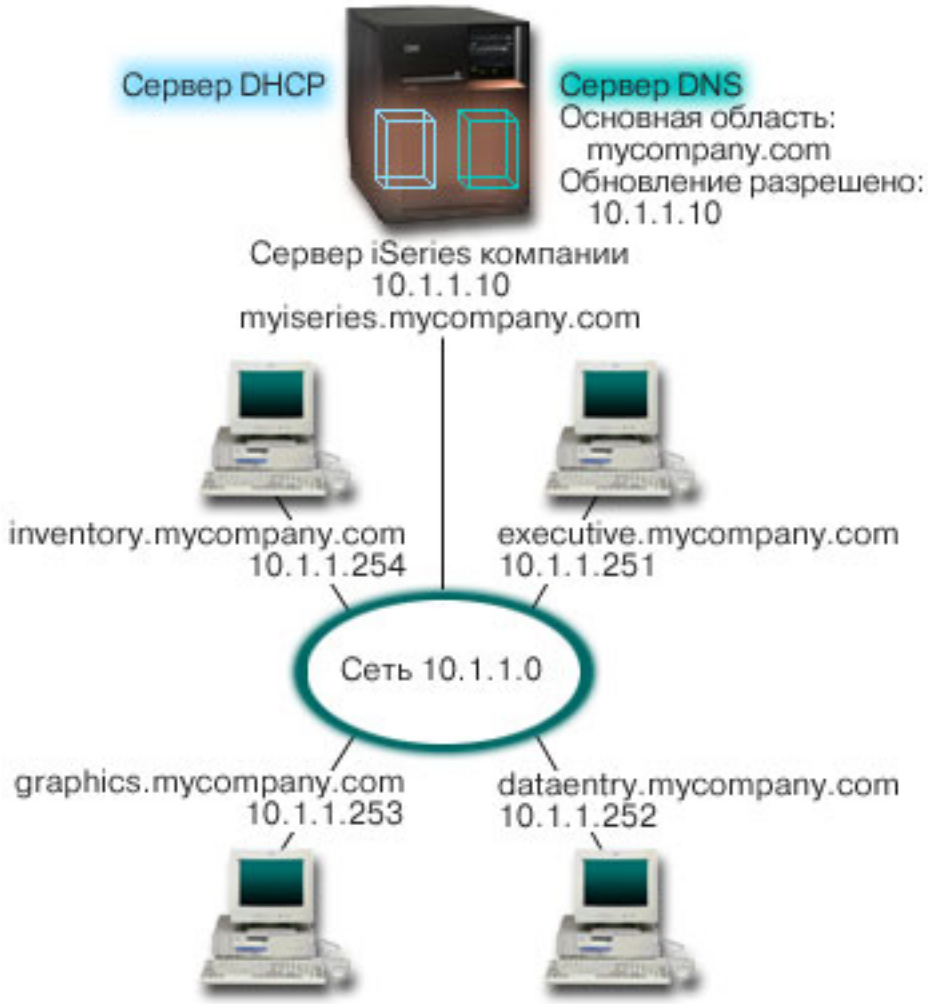

Рисунок 4. Серверы DNS и DHCP, расположенные в одной системе System i

В предыдущих версиях серверы DHCP и DNS не были связаны друг с другом. Когда сервер DHCP присваивал клиенту новый IP-адрес, администратор должен был вручную обновлять соответствующие записи на сервере DNS. В данном примере при обновлении IP-адреса сервера графических файлов сервером DHCP клиенты не смогут подключить сетевой диск, так как в записях DNS будет храниться старый IP-адрес сервера.

В версии i5/OS сервер DNS основан на стандарте BIND 9, поэтому вы можете разрешить динамическое обновление информации об области, чтобы записи DNS автоматически обновлялись сервером DHCP при изменении адреса. Например, когда истечет время выделения адреса для сервера графических файлов, и сервер DHCP присвоит ему новый IP-адрес 10.1.1.250, соответствующие записи DNS будут автоматически изменены. В результате сразу после изменения адреса клиенты получат от сервера DNS правильный ответ на запрос об IP-адресе, связанном с именем хоста сервера графических файлов.

Для настройки функции динамического обновления области DNS выполните следующие действия:

- Определите динамическую область

  Динамическую область нельзя обновлять вручную во время работы сервера. Это может привести к конфликту с поступившими запросами на динамическое обновление. Для внесения обновлений вручную нужно остановить сервер. Однако при этом все запросы на динамическое обновление, полученные во время простоя сервера, не будут обработаны. В связи с этим рекомендуется создать отдельную динамическую область, выбрав ее таким образом, чтобы записи DNS нужно было редко изменять

вручную. Дополнительная информация о настройке областей для работы с функцией динамического обновления информации приведена в разделе Определение структуры домена.

- Настройте опцию allow-update

  Если для области задана опция allow-update, то она считается динамической областью. Эта опция устанавливается индивидуально для каждой области. Запросы на динамическое обновление области будут приниматься сервером только в том случае, если для этой области задана опция allow-update. В данном примере опцию allow-update обязательно нужно установить для области mycompany.com. Остальные области могут быть настроены как статические или как динамические по вашему усмотрению.

- Настройте функцию динамического обновления на сервере DHCP

  Серверу DHCP необходимо предоставить права на динамическое обновление записей DNS при изменении IP-адреса.

- Настройте параметры обновления информации на вспомогательном сервере

  Для своевременного обновления информации на вспомогательных серверах настройте функцию NOTIFY на сервере DNS. В результате сервер DNS будет отправлять вспомогательным серверам сообщения обо всех изменениях записей области mycompany.com. Кроме того, настройте функцию передачи измененной информации об области (IXFR), для того чтобы вспомогательные серверы, поддерживающие IXFR, загружали только измененную информацию об области, а не всю информацию целиком.

Если вы планируете настроить серверы DNS и DHCP в разных системах, следует учесть дополнительные требования к конфигурации сервера DHCP.

Понятия, связанные с данным

“Динамическое обновление данных DNS” на стр. 6
i5/OS Система имен доменов (DNS) с применением стандарта BIND 9 поддерживает динамическое обновление. Запросы на динамическое обновление отправляются некоторыми внешними службами, в частности, службой Протокола динамической настройки хостов (DHCP). Для динамического обновления можно использовать также и инструменты клиента, например программу динамического обновления (NSUPDATE).

Задачи, связанные с данной

Настройка функции динамического обновления DNS на сервере DHCP

Ссылки, связанные с данной

Пример: Серверы DNS и DHCP, расположенные в разных системах System i

Пример: Разделение областей ответственности DNS в сети с брандмауэром путем настройки двух серверов DNS в одной системе System i

В этом примере описана настройка сервера DNS в сети с брандмауэром, который защищает данные внутренних хостов от внешних пользователей, не ограничивая доступ внутренних пользователей к Internet. Такая конфигурация защищает данные путем настройки двух серверов DNS в одной системе System i.

На приведенном ниже рисунке показана схема небольшой подсети, для защиты которой применяется брандмауэр. Предположим, что в корпоративной сети есть внутренняя подсеть с зарезервированным пространством IP-адресов, и внешняя подсеть, которая доступна внешним пользователям. Для работы внутренним пользователям необходимо обмениваться почтой с пользователями внешней сети и подключаться к внешним хостам. Кроме того, у внутреннего сервера DNS должен быть доступ только к некоторым внутренним областям, которые недоступны внешним хостам. В то же время внешним серверам DNS также запрещается доступ к внутренней сети.

Для сервера DNS системы i5/OS, основанного на BIND 9, можно реализовать это двумя способами. Первый способ заключается в настройке двух экземпляров сервера DNS в одной и той же системе System i: один для внутренней сети, а другой - для общего домена. Этот способ описан в данном примере. Второй способ заключается в использовании создания представлений, которые предусмотрены в BIND 9. Он описан в

примере разделения областей ответственности DNS в сети с брандмауэром с помощью представлений.

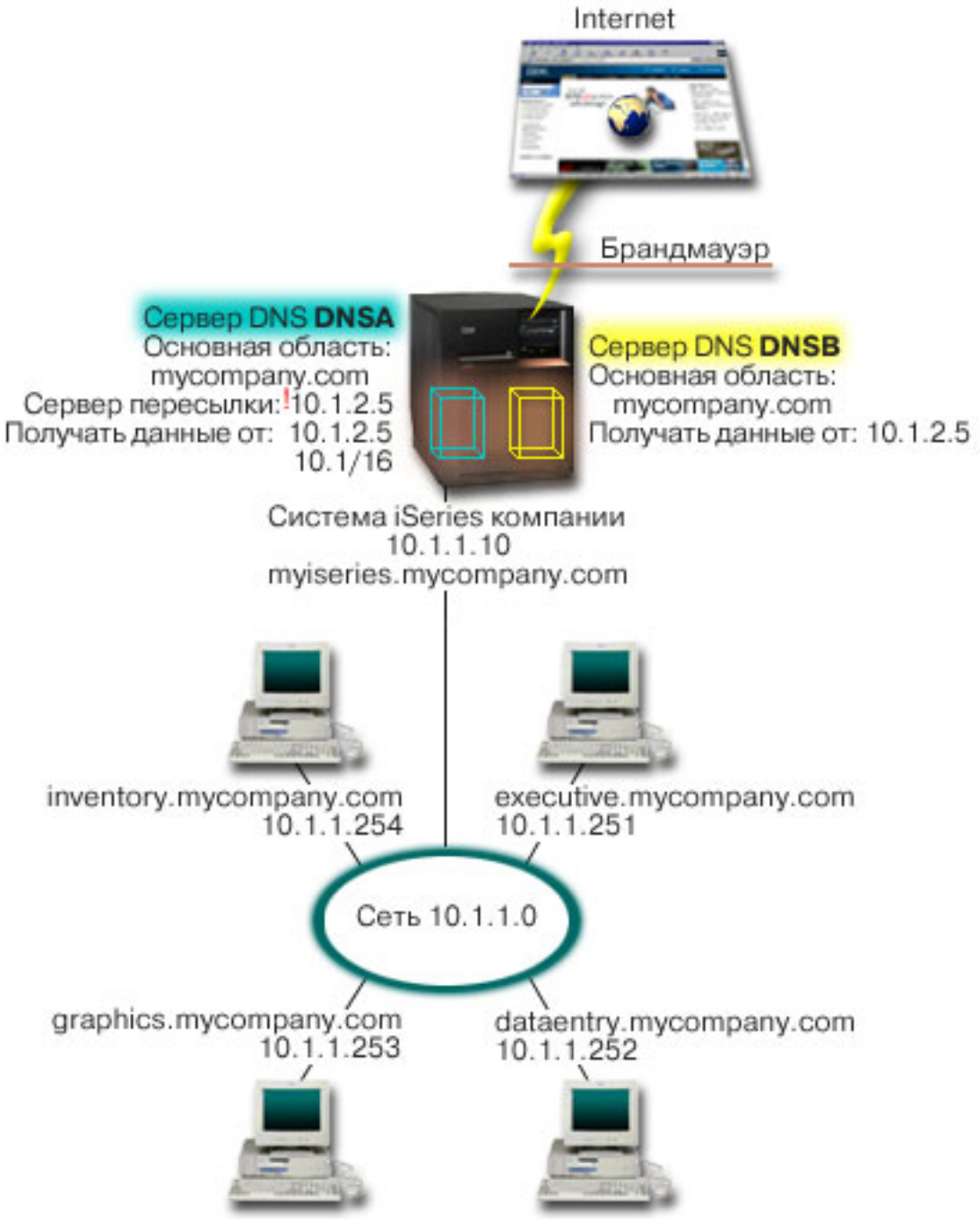

Рисунок 5. Пример: Разделение областей ответственности DNS в сети с брандмауэром путем настройки двух серверов DNS в одной системе System i

В качестве основной области внешнего сервера, DNSB, выбирается mycompany.com. Однако информация об этой области будет включать только те записи о ресурсах, которые относятся к внешнему домену. Основной областью внутреннего сервера, DNSA, также служит mycompany.com, однако информация об этой области содержит только те записи о ресурсах, которые относятся к внутренней сети. В качестве адреса сервера пересылки выбирается 10.1.2.5. В результате сервер DNSA будет пересылать запросы, которые он не может обработать, серверу DNSB.

Если вы хотите обеспечить целостность брандмауэра или принять другие меры защиты, настройте опцию listen-on для защиты внутренних данных. Для этого разрешите внутренним хостам отправлять внутреннему серверу только те запросы, которые относятся к внутренней области mycompany.com. Для работы описанной конфигурации необходимо, чтобы внутренние клиенты отправляли запросы только серверу DNSA. Для настройки DNS с разделенной областью ответственности рекомендуется настроить следующие параметры:

- Рабочий адрес

  В других примерах в системе System i работает только один сервер DNS. Он получал запросы через все интерфейсы IP-адресов системы. Если в системе System i создано несколько серверов DNS, для каждого из них нужно задать набор IP-адресов интерфейсов, через которые они будут получать запросы. Эти наборы не должны пересекаться. В данном случае предположим, что все запросы, поступающие через брандмауэр, будут отправляться через интерфейс 10.1.2.5. Эти запросы должны быть отправлены внешнему серверу. Следовательно, сервер DNSB должен работать с IP-адресом 10.1.2.5. Внутренний сервер, DNSA, может принимать запросы через любой интерфейс 10.1.x.x, за исключением 10.1.2.5. Для того чтобы исключить этот адрес, укажите его в списке адресов для сравнения перед разрешенным префиксом адреса.

- Порядок элементов в списке адресов для сравнения

  Всегда применяется тот элемент адреса, который был найден первым. Например, для того чтобы разрешить прием запросов от всех адресов 10.1.x.x, за исключением 10.1.2.5, элементы в списке должны быть расположены в следующем порядке: (!10.1.2.5; 10.1/16). В данном случае для адреса 10.1.2.5 первой будет найдена запись, запрещающая доступ.

  Если элементы будут стоять в обратном порядке (10.1/16; !10.1.2.5), то для IP-адреса 10.1.2.5 первой будет найдена запись, разрешающая доступ. Поскольку остальные записи списка не проверяются, запрос от этого адреса будет принят.

Ссылки, связанные с данной

“Новые возможности BIND 9” на стр. 8
Стандарт BIND 9 подобен стандарту BIND 8. Тем не менее, в нем предусмотрен ряд новых возможностей, позволяющих повысить производительность сервера Системы имен доменов (DNS), например представления.

“Пример: Разделение областей ответственности DNS в сети с брандмауэром с помощью представлений”
В этом примере описана настройка сервера DNS в сети с брандмауэром, который защищает данные внутренних хостов от внешних пользователей, не ограничивая доступ внутренних пользователей к Internet, с помощью возможности *view*, предусмотренной в BIND 9.

Пример: Разделение областей ответственности DNS в сети с брандмауэром с помощью представлений

В этом примере описана настройка сервера DNS в сети с брандмауэром, который защищает данные внутренних хостов от внешних пользователей, не ограничивая доступ внутренних пользователей к Internet, с помощью возможности *view*, предусмотренной в BIND 9.

На приведенном ниже рисунке показана схема небольшой подсети, для защиты которой применяется брандмауэр. Предположим, что в корпоративной сети есть внутренняя подсеть с зарезервированным пространством IP-адресов, и внешняя подсеть, которая доступна внешним пользователям. Для работы внутренним пользователям необходимо обмениваться почтой с пользователями внешней сети и подключаться к внешним хостам. Кроме того, у внутреннего сервера DNS должен быть доступ только к некоторым внутренним областям, которые совершенно недоступны внешним хостам. В то же время внешним серверам DNS также запрещается доступ к внутренней сети.

Для сервера DNS системы i5/OS, основанного на BIND 9, можно реализовать это двумя способами. В этом примере описан способ настройки сервера DNS с двумя различными представлениями, которые принимают различные запросы: один для внутренней сети, а другой - для общего домена. Второй способ заключается в настройке двух экземпляров сервера DNS в одной и той же системе System i. Он описан в примере разделения областей ответственности DNS в сети с брандмауэром с использованием двух серверов DNS.

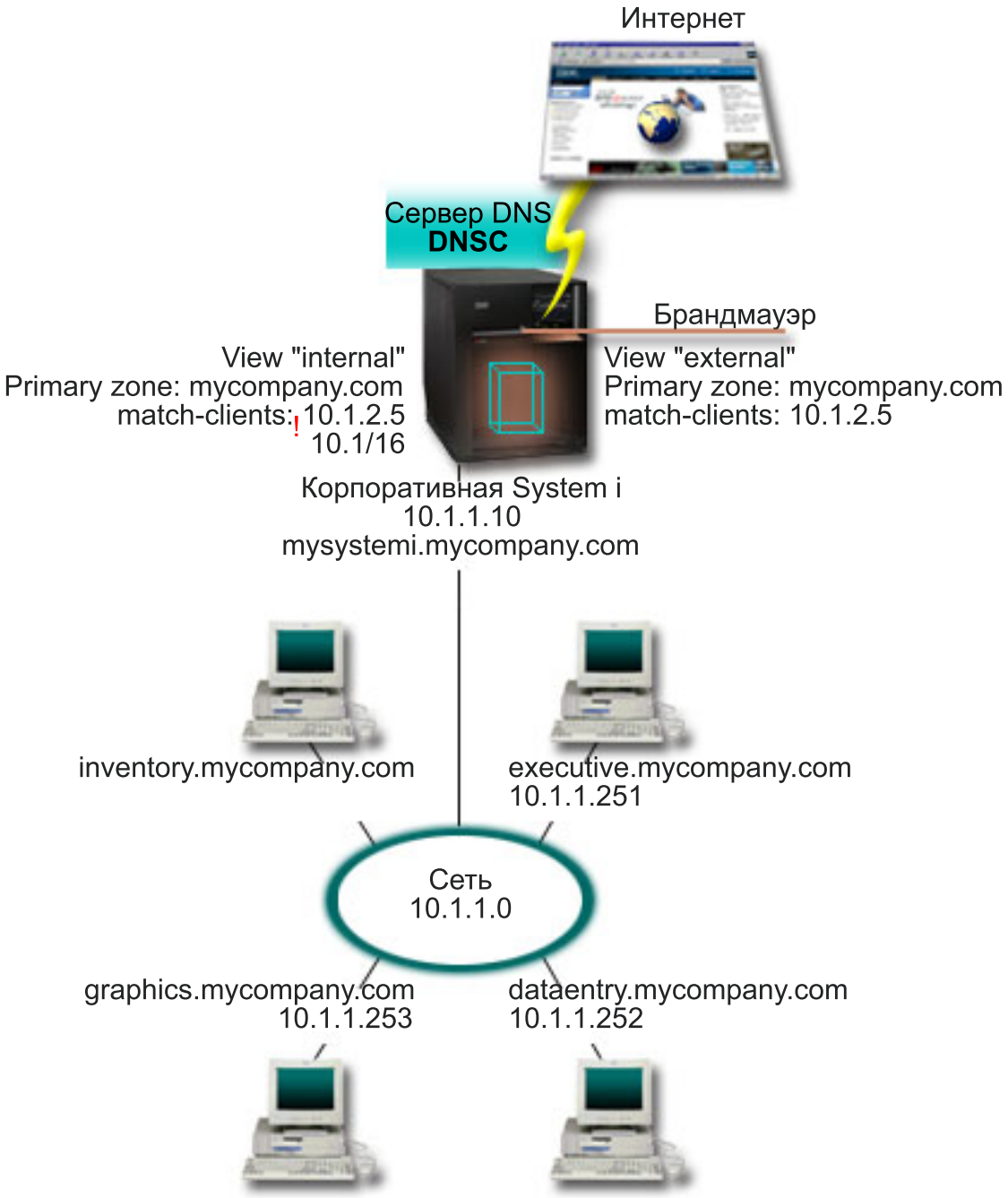

Рисунок 6. Разделение областей ответственности DNS в сети с брандмауэром с помощью представлений

На сервере DNS, DNSC, определены два представления, которые называются *внешнее* и *внутреннее*. Основной областью *внешнего* представления служит mycompany.com, которая включает в себя только те записи о ресурсах, которые предназначены для того, чтобы быть частью общего домена. Основной областью *внутреннего* представления также является mycompany.com, но она содержит только записи о ресурсах, которые относятся к внутренней сети.

Если вы хотите обеспечить целостность брандмауэра или принять другие меры защиты, используйте оператор match-clients для защиты внутренних данных. Для этого разрешите внутренним хостам отправлять

внутреннему представлению только те запросы, которые относятся к внутренней области mycompany.com. Для настройки DNS с разделенной областью ответственности рекомендуется настроить следующие параметры:

- Match-clients

  Выражение match-clients в операторе представления принимает в качестве аргумента список соответствий. Значения настройки, определенные в окружающем представлении, видны только для тех IP-адресов запросов, которые включены в список соответствий адресов. Если IP-адрес запроса совпадает с несколькими записями match-clients в различных операторах представления, то применяется первый оператор. В данном случае предположим, что все запросы, поступающие через брандмауэр, будут отправляться через интерфейс 10.1.2.5. Эти запросы должны обрабатываться информацией об области во внешнем представлении. Поэтому в качестве match-clients для внешнего представления установлен адрес 10.1.2.5. Внутреннее представление может принимать запросы через любой интерфейс 10.1.x.x, за исключением 10.1.2.5. Для того чтобы исключить этот адрес, укажите его в списке адресов для сравнения перед разрешенным префиксом адреса.

- Порядок элементов в списке адресов для сравнения

  Всегда применяется тот элемент адреса, который был найден первым. Например, для того чтобы разрешить прием запросов от всех адресов 10.1.x.x, за исключением 10.1.2.5, элементы в списке должны быть расположены в следующем порядке: (!10.1.2.5; 10.1/16). В данном случае для адреса 10.1.2.5 первой будет найдена запись, запрещающая доступ.

  Если элементы будут стоять в обратном порядке (10.1/16; !10.1.2.5), то для IP-адреса 10.1.2.5 первой будет найдена запись, разрешающая доступ. Поскольку остальные записи списка не проверяются, запрос от этого адреса будет принят.

Ссылки, связанные с данной

“Пример: Разделение областей ответственности DNS в сети с брандмауэром путем настройки двух серверов DNS в одной системе System i” на стр. 20
В этом примере описана настройка сервера DNS в сети с брандмауэром, который защищает данные внутренних хостов от внешних пользователей, не ограничивая доступ внутренних пользователей к Internet. Такая конфигурация защищает данные путем настройки двух серверов DNS в одной системе System i.

Планирование DNS

Существует множество вариантов настройки DNS. Перед настройкой сервера DNS нужно заранее продумать, какие функции он будет выполнять в сети. Кроме того, необходимо предварительно спланировать структуру сети, нагрузку на сервер и параметры его защиты.

Определение прав доступа для работы с DNS

Администратору сервера DNS должны быть предоставлены особые права доступа. Следует тщательно продумать, какие именно права доступа можно предоставить администратору без ущерба для защиты сервера.

При настройке сервера DNS следует принять меры по защите конфигурации сервера. Укажите, каким пользователям разрешено изменять эту конфигурацию.

Для настройки и обслуживания сервера DNS администратору системы достаточно минимальных прав доступа. Если администратору будут предоставлены права доступа ко всем объектам, то он сможет выполнять любые задачи по администрированию сервера DNS. Пользователям, отвечающим за настройку сервера DNS, рекомендуется предоставить права администратора защиты и права доступа ко всем объектам (*ALLOBJ). Для предоставления этих прав доступа воспользуйтесь System i Navigator. За дополнительной информацией по этому вопросу обратитесь к разделу Предоставление прав доступа администратору сервера DNS электронной справки по серверу DNS.

Примечание: Если профайлу администратора не предоставлены права доступа ко всем объектам, то ему должны быть предоставлены права доступа ко всем каталогам и файлам конфигурации DNS.

Ссылки, связанные с данной

"Работа с файлами конфигурации DNS" на стр. 35
Для создания экземпляров сервера DNS в системе System i и работы с ними применяется служба DNS i5/OS. Функции для работы с файлами конфигурации DNS предусмотрены в Навигаторе System i NavigatorSystem i Navigator

Определение структуры домена

Перед настройкой домена необходимо определить, каким образом он будет разбит на области.

Заранее спланируйте, каким образом домен или субдомен будет разделен на области, каким образом лучше обрабатывать запросы, будет ли сервер DNS подключен к Internet, и каким образом сервер DNS будет работать через брандмауэр. Последовательно рассмотрите несколько вариантов настройки сервера. За более подробными сведениями обратитесь к дополнительным источникам информации, например, к книге O'Reilly DNS and BIND.

Если вы создадите динамическую область, вы не сможете обновлять эту область во время работы сервера. Это может привести к конфликту с поступившими запросами на динамическое обновление. Для внесения изменений вручную остановите сервер, обновите информацию об области, а затем перезапустите сервер. При этом запросы на динамическое обновление, полученные во время простоя сервера DNS, обработаны не будут. По этой причине рекомендуется настроить две области: статическую и динамическую. Для этого нужно создать две отдельные области или определить субдомен для тех клиентов, записи о которых будут обновляться динамически, например, dynamic.mycompany.com.

Для настройки систем на сервере DNS системы i5/OS предусмотрен графический интерфейс. Названия некоторых объектов в этом интерфейсе отличаются от тех, которые принято использовать в других публикациях. Если при планировании конфигурации DNS вы будете обращаться к другим источникам информации, учтите следующее:

- Все области и объекты, определенные в системе System i, расположены в папках Области прямого преобразования и Области обратного преобразования. Области прямого преобразования применяются для преобразования имен хостов в IP-адреса, например, с помощью записей типа A и AAAA. Области обратного преобразования применяются для преобразования IP-адресов в имена хостов, например, с помощью записей PTR.
- На сервере DNS системы i5/OS могут быть определены *основные* и *вспомогательные области*.
- Термин *подобласть* аналогичен *субдомену*. Дочерней областью называется подобласть, права на управление которой переданы одному или нескольким серверам имен.

Планирование мер защиты

В службе DNS предусмотрен ряд средств защиты, позволяющих ограничить доступ внешних пользователей к серверу.

Списки адресов для сравнения

Список адресов для сравнения применяется сервером DNS для управления доступом внешних клиентов к некоторым функциям DNS. В таком списке могут быть заданы IP-адреса, адреса подсети (с помощью префикса IP), либо ключи Подписи транзакции (TSIG). В списке адресов для сравнения перечисляются объекты, которым разрешен или запрещен доступ к функциям сервера. Если вы планируете многократно использовать список адресов для сравнения, сохраните его как список управления доступом (ACL). Если вам впоследствии потребуется этот список, вам нужно будет указать только имя ACL.

Порядок элементов в списке адресов для сравнения

Всегда применяется тот элемент адреса, который был найден первым. Следовательно, для того чтобы разрешить доступ для всех хостов сети 10.1.1.x, за исключением 10.1.1.5, элементы в списке должны быть расположены в следующем порядке: (!10.1.1.5; 10.1.1/24). В этом случае для адреса 10.1.1.5 первой будет найдена запись, запрещающая доступ.

Если элементы будут стоять в обратном порядке (10.1.1/24; !10.1.1.5), то для IP-адреса 10.1.1.5 первой будет найдена запись, разрешающая доступ. Поскольку остальные записи списка не проверяются, хосту будет разрешен доступ к функции сервера.

Опции управления доступом

Сервер DNS позволяет настроить ряд ограничений доступа, в частности, задать список клиентов, которым разрешено отправлять запросы на динамическое обновление, запрашивать информацию и загружать информацию об области. Для ограничения доступа к серверу с помощью списков управления доступом предусмотрены следующие опции:

allow-update
Включите эту опцию, для того чтобы сервер DNS принимал запросы на динамическое обновление информации от внешних клиентов.

allow-query
Указывает, каким хостам разрешено отправлять запросы к этому серверу. По умолчанию доступ к серверу предоставляется всем хостам.

allow-transfer
Указывает, каким хостам разрешено загружать информацию об области с сервера. По умолчанию это разрешено всем хостам.

allow-recursion
Указывает, каким хостам разрешено отправлять рекурсивные запросы данному серверу. По умолчанию это разрешено всем хостам.

blackhole
Задает список адресов хостов, от которых сервер не принимает запросы и которым сервер не пересылает запросы для обработки. Сервер не отвечает на запросы, поступающие от указанных хостов.

Необходимо тщательно спланировать меры по защите сервера DNS. Помимо перечисленных ниже разделов с рекомендациями по защите, существует множество других источников информации о защите сервера DNS и системы System i. В частности, такая информация приведена в разделе System i и Internet. Подробную информацию о защите DNS можно найти в книге *DNS and BIND*.

Понятия, связанные с данным

Защита системы System i при работе с Internet

Ссылки, связанные с данной

“Новые возможности BIND 9” на стр. 8
Стандарт BIND 9 подобен стандарту BIND 8. Тем не менее, в нем предусмотрен ряд новых возможностей, позволяющих повысить производительность сервера Системы имен доменов (DNS), например представления.

Требования DNS

В этом разделе приведен список программного обеспечения, которое требуется для работы DNS в системе System i.

DNS, компонент 31, не устанавливается автоматически при установке операционной системы. Вы должны самостоятельно установить DNS. Новая реализация сервера DNS, предусмотренная в i5/OS, основана на общепринятом стандарте BIND 9. В предыдущих выпусках OS/400 сервер DNS был основан на стандарте BIND 8.2.5. Этот стандарт по-прежнему поддерживается в i5/OS.

После установки DNS вам потребуется обновить сервер DNS с BIND 4 или 8 до BIND 9 и настроить его. Также вам потребуется установить PASE i5/OS, который является компонентом 33 i5/OS. После установки PASE i5/OSSystem i Navigator автоматически настроит сервер на основе текущей реализации BIND.

Если для динамического обновления информации на локальном сервере DNS вы планируете настроить Протокол динамической настройки хостов (DHCP) в другой системе, то в ней также необходимо установить компонент 31. Для динамического обновления информации сервер DHCP применяет программные интерфейсы, которые предоставляются компонентом 31.

Понятия, связанные с данным

i5/OS PASE

"Настройка Системы имен доменов"
Для настройки серверов имен и преобразования запросов, не относящихся к вашему домену, можно использовать System i Navigator.

Ссылки, связанные с данной

"Новые возможности BIND 9" на стр. 8
Стандарт BIND 9 подобен стандарту BIND 8. Тем не менее, в нем предусмотрен ряд новых возможностей, позволяющих повысить производительность сервера Системы имен доменов (DNS), например представления.

Определение наличия установленной службы DNS

Для того чтобы узнать, установлена ли служба DNS в системе, выполните следующие действия.

1. В командной строке введите `GO LICPGM` и нажмите Enter.
2. Введите `10` (Показать установленные лицензионные программы) и нажмите Enter.
3. Найдите запись **5761SS1 Domain Name System** (Компонент 31) Если служба DNS установлена, то в поле Состояние будет указано значение `*COMPATIBLE`, как показано ниже:

```
Программа   Состояние          Описание
5761SS1    *COMPATIBLE         Domain Name System
```

4. Для выхода из меню нажмите F3.

Установка Системы имен доменов

Для того, чтобы установить DNS, выполните следующие действия.

1. В командной строке введите `GO LICPGM` и нажмите Enter.
2. Введите `11` (Установить лицензионные программы) и нажмите Enter.
3. В поле **Опция** напротив записи `Domain Name System` введите `1` (Установить) и нажмите Enter.
4. Нажмите Enter еще раз для подтверждения установки.

Настройка Системы имен доменов

Для настройки серверов имен и преобразования запросов, не относящихся к вашему домену, можно использовать System i Navigator.

Перед настройкой сервера DNS ознакомьтесь с системными требованиями DNS и установите все требуемые компоненты DNS.

Понятия, связанные с данным

“Требования DNS” на стр. 26
В этом разделе приведен список программного обеспечения, которое требуется для работы DNS в системе System i.

Управление доступом к Системе имен доменов в System i Navigator

Ниже приведены инструкции по работе с интерфейсом для настройки DNS, предусмотренным в System i Navigator.

Если вы используете PASE i5/OS, то вы сможете настроить серверы DNS на основе BIND 9.

Если вы впервые настраиваете сервер DNS, выполните следующие действия:

1. В System i Navigator, разверните список ***ваша система*** → **Сеть** → **Серверы** → **DNS**.
2. Щелкните правой кнопкой мыши на пункте **DNS** и выберите **Создать конфигурацию**.

Понятия, связанные с данным

Знакомство с Навигатором System i

Настройка серверов имен

Вы можете создать несколько экземпляров серверов имен. В этом разделе приведены инструкции по настройке сервера имен.

DNS i5/OS с использованием BIND 9 поддерживает множественные экземпляры сервера имен. Ниже описана процедура создания экземпляра сервера имен, включающая настройку свойств и областей сервера.

Для того чтобы создать дополнительный экземпляр сервера, повторите описанные процедуры. Свойства экземпляров сервера не обязательно должны совпадать - для каждого из них вы можете задать свой уровень отладки, опцию автоматического запуска и т.д. Для каждого экземпляра сервера создаются свои файлы конфигурации.

Ссылки, связанные с данной

“Работа с файлами конфигурации DNS” на стр. 35
Для создания экземпляров сервера DNS в системе System i и работы с ними применяется служба DNS i5/OS. Функции для работы с файлами конфигурации DNS предусмотрены в Навигаторе System i NavigatorSystem i Navigator

Создание экземпляра сервера имен

Мастер Создать конфигурацию DNS поможет вам создать экземпляр сервера DNS.

Для запуска мастера **Создать конфигурацию сервера DNS** выполните следующие действия:

1. В System i Navigator, разверните список ***ваша система*** → **Сеть** → **Серверы** → **DNS**.
2. В левой панели щелкните правой кнопкой мыши на пункте **DNS** и выберите **Создать сервер имен**.
3. Выполните инструкции мастера по настройке сервера.

В окнах мастера потребуется указать следующие значения:

Имя сервера DNS:
Укажите имя сервера DNS. Оно может содержать не более 5 символов, первым из которых должна быть буква (A-Z). Если вы планируете создать несколько серверов, присвойте им различные имена. Иногда это имя называют именем экземпляра сервера DNS.

Рабочие IP-адреса:
Два сервера DNS не могут работать на одном и том же IP-адресе. По умолчанию сервер работает со всеми IP-адресами. Однако если в системе будет работать несколько экземпляров серверов, ни один из них не должен работать со всеми IP-адресами. В противном случае они не смогут работать одновременно. В этом случае для каждого сервера необходимо указать свой список IP-адресов.

Корневые серверы:

Загрузите список корневых серверов Internet по умолчанию, либо укажите собственные корневые серверы, например, внутренние корневые серверы для своей корпоративной сети.

Примечание: Список корневых серверов Internet следует загружать только в том случае, если сервер подключен к Internet и будет применяться для получения произвольных имен Internet.

Запуск сервера:

Укажите, следует ли автоматически запускать сервер вместе с TCP/IP. Если в системе создано несколько экземпляров сервера, каждый из них запускается и останавливается независимо от остальных.

Настройка свойств сервера DNS

Во время создания сервера имен вы можете настроить его свойства, в том числе разрешить обновление информации на сервере и задать уровни отладки. Эти значения относятся только к тому экземпляру сервера, с которым вы в данный момент работаете.

Для того чтобы изменить свойства экземпляра сервера DNS, выполните следующие действия:

1. В System i Navigator, разверните список ***ваша система*** → **Сеть** → **Серверы** → **DNS**.
2. В правой панели щелкните правой кнопкой мыши на ***значке сервера DNS*** и выберите пункт **Конфигурация**.
3. В окне Конфигурация сервера DNS щелкните правой кнопкой мыши на значке **сервера DNS** и выберите пункт **Свойства**.
4. Измените соответствующие свойства требуемым образом.

Настройка областей сервера имен

После настройки экземпляра сервера DNS необходимо настроить области сервера имен.

Для настройки областей сервера выполните следующие действия:

1. В System i Navigator, разверните список ***ваша система*** → **Сеть** → **Серверы** → **DNS**.
2. В правой панели щелкните правой кнопкой мыши на ***значке сервера DNS*** и выберите пункт **Конфигурация**.
3. В окне Конфигурация DNS выберите тип области, которую требуется создать, щелкнув правой кнопкой мыши либо на значке папки **Область прямого преобразования**, либо на значке папки **Область обратного преобразования**.
4. Выполните инструкции мастера по созданию области.

Понятия, связанные с данным

“Получение информации от внешних серверов DNS” на стр. 31
Сервер DNS может отвечать на запросы о той области, которая для него создана.

Задачи, связанные с данной

“Настройка функции динамического обновления на сервере DNS” на стр. 30
Серверы DNS, поддерживающие BIND 9, могут принимать запросы на динамическое обновление информации об области от различных служб. В этом разделе приведены инструкции по настройке функции динамического обновления на сервере DNS.

“Импорт файлов DNS” на стр. 30
На сервер DNS можно импортировать файлы с информацией об областях. В этом разделе описана процедура создания области на основе существующего файла конфигурации, позволяющая значительно сэкономить время при создании области.

Ссылки, связанные с данной

“Основные сведения об областях” на стр. 3
Вся информация Системы имен доменов (DNS) поделена на наборы данных, называемые *областями*. Каждый из этих наборов является специфическим типом области.

Настройка представлений сервера имен

Одной из возможностей, которые предоставляет BIND 9, является оператор *view*, который позволяет одиночному экземпляру DNS по-разному отвечать на запрос в зависимости от того, откуда направлен запрос, например из Internet или внутренней сети. Одно из практических применений представлений - разделение настроек DNS без использования нескольких серверов DNS.

Для настройки представлений сервера выполните следующие действия:

1. В System i Navigator, разверните список ***ваша система*** → **Сеть** → **Серверы** → **DNS**.
2. В правой панели щелкните правой кнопкой мыши на ***значке сервера DNS*** и выберите пункт **Конфигурация**.
3. В окне Конфигурация сервера DNS щелкните правой кнопкой мыши на значке **Представления** и выберите пункт **Создать представление**.
4. Выполните инструкции мастера по созданию области.

Настройка функции динамического обновления на сервере DNS

Серверы DNS, поддерживающие BIND 9, могут принимать запросы на динамическое обновление информации об области от различных служб. В этом разделе приведены инструкции по настройке функции динамического обновления на сервере DNS.

При создании динамических областей следует учесть структуру сети. Если некоторые компоненты домена по-прежнему будут обновляться вручную, рекомендуется поделить домен на статическую и динамическую области. Для того чтобы вручную обновить динамическую область, вам потребуется остановить сервер, отвечающий за эту область, и перезапустить его после внесения всех изменений. При завершении работы сервера выполняется обновление базы данных области с применением всех динамических обновлений, внесенных с момента первой загрузки информации об области из базы данных. Если вы не остановите сервер, то он запишет новые данные поверх всех изменений, которые внесены вручную. Однако завершив работу сервера, вы рискуете потерять те динамические обновления, которые были сделаны во время простоя сервера.

Динамическая область отличается от остальных тем, что в ней определены объекты в операторе allow-update. Для того чтобы определить такие объекты, выполните следующие действия:

1. В System i Navigator, разверните список ***ваша система*** → **Сеть** → **Серверы** → **DNS**.
2. В правой панели щелкните правой кнопкой мыши на ***значке сервера DNS*** и выберите пункт **Конфигурация**.
3. В окне Конфигурация DNS разверните значок **Область прямого преобразования** или **Область обратного преобразования**.
4. Щелкните правой кнопкой мыши на основной области, в которую нужно внести изменения, и выберите пункт **Свойства**.
5. На странице Свойства основной области щелкните на вкладке **Опции**.
6. На странице Опции разверните **Управление доступом** → **allow-update**.
7. Для проверки запросов на обновление сервер DNS применяет список адресов для сравнения. Для добавления объектов в этот список выберите тип элемента списка и нажмите кнопку **Добавить**. Вы можете добавить IP-адрес, префикс IP, список управления доступом или ключ.
8. После изменения списка адресов для сравнения нажмите кнопку **OK**, чтобы закрыть окно Опции.

Задачи, связанные с данной

“Настройка областей сервера имен” на стр. 29
После настройки экземпляра сервера DNS необходимо настроить области сервера имен.

Настройка функции динамического обновления DNS на сервере DHCP

Импорт файлов DNS

На сервер DNS можно импортировать файлы с информацией об областях. В этом разделе описана процедура создания области на основе существующего файла конфигурации, позволяющая значительно сэкономить время при создании области.

Основную область можно создать путем импорта файла с информацией об области, поддерживающего синтаксис BIND. Этот файл должен быть расположен в каталоге Интегрированной файловой системы. После импорта файла с информацией об области DNS проверит, что он не содержит ошибок, и добавит его имя в файл named.conf для соответствующего экземпляра сервера.

Для того чтобы импортировать файл с информацией об области, выполните следующие действия:

1. В System i Navigator, разверните список ***ваша система*** → **Сеть** → **Серверы** → **DNS**.
2. На правой панели дважды щелкните на значке экземпляра сервера DNS, для которого нужно импортировать область.
3. В левой панели окна Настройки DNS щелкните правой кнопкой мыши на значке **сервера DNS** и выберите опцию **Импортировать область**.
4. Выполните инструкции мастера по импорту основной области.

Задачи, связанные с данной

"Настройка областей сервера имен" на стр. 29
После настройки экземпляра сервера DNS необходимо настроить области сервера имен.

Проверка записей

Функция Импортировать данные домена проверяет все записи импортируемого файла.

Неправильные записи можно исправить по окончании импорта, перейдя на страницу свойств Прочие записи импортированной области.

Notes:

1. Импорт большого основного домена может занять несколько минут.
2. Функция импорта данных домена не поддерживает директиву include. При проверке строки с директивой include считаются неправильными.

Получение информации от внешних серверов DNS

Сервер DNS может отвечать на запросы о той области, которая для него создана.

Корневые серверы необходимы для работы сервера DNS, напрямую подключенного к Internet или большой внутренней сети. Для ответа на запросы о хостах, не входящих в его домен, сервер DNS обращается к корневому серверу.

В сети Internet, если серверу DNS нужно получить дополнительную информацию, он обращается к корневым серверам. Корневые серверы передают запрос сервера DNS выше по иерархической структуре до тех пор, пока нужная информация не будет найдена или не выяснится, что она отсутствует.

Список корневых серверов по умолчанию для System i Navigator

Корневые серверы должны применяться в том случае, если система подключена к Internet и вы хотите, чтобы сервер DNS отправлял в Internet запросы о хостах, которые он не может обработать самостоятельно. В System i Navigator определен ряд корневых серверов Internet, применяемых по умолчанию. Данный список действителен для выпуска System i Navigator. Для того чтобы убедиться, что этот список не устарел, сравните его со списком серверов, приведенном на Web-сайте InterNIC. При необходимости обновите список корневых серверов.

Получение адресов корневых серверов Internet

Адреса корневых серверов иногда меняются, и обновление их списка на сервере локального домена является обязанностью администратора DNS. Текущий список адресов корневых серверов Internet расположен на сайте InterNIC. Для получения этого списка выполните следующие действия:

1. Войдите на сервер InterNIC FTP.INTERNIC.NET или RS.INTERNIC.NET по протоколу передачи файлов (FTP) под анонимной учетной записью.
2. Загрузите файл /domain/named.root
3. Сохраните файл в каталоге /QOpenSys/QIBM/ProdData/OS400/DNS/ROOT.FILE

Сервер DNS, защищенный брандмауэром, может работать без корневых серверов. Такой сервер DNS отвечает на запросы, пользуясь только записями из собственной базы данных основного домена и кэша. Запросы, касающиеся внешних сайтов, он может отправлять серверу DNS, расположенному на брандмауэре, где должен быть установлен сервер пересылки.

Внутренние корневые серверы

Если сервер DNS расположен в большой внутренней сети, то рекомендуется настроить внутренние корневые серверы. Если сервер DNS не будет обращаться к серверам Internet, то список серверов Internet по умолчанию загружать не нужно. Вместо этого необходимо задать имена внутренних корневых серверов, с помощью которых сервер DNS будет выполнять запросы о хостах, не относящихся к его домену.

Задачи, связанные с данной

“Настройка областей сервера имен” на стр. 29
После настройки экземпляра сервера DNS необходимо настроить области сервера имен.

Управление Системой имен доменов

К управлению сервером Системы имен доменов (DNS) относятся проверка правильности работы DNS, сбор информации о его производительности и выполнение необходимых действий над данными и файлами DNS.

Проверка правильности работы Системы имен доменов

Инструмент Domain Information Groper (DIG) помогает собирать информацию с сервера Системы имен доменов (DNS) и тестировать его ответы. DIG можно использовать для проверки правильности работы сервера DNS.

Запросите имя хоста, связанное с циклическим IP-адресом (127.0.0.1). Вы должны получить имя хоста localhost. Кроме того, проверьте, что сервер правильно отвечает на запросы о получении имен хостов, определенных в записях сервера. Там самым вы убедитесь, что экземпляр сервера работает правильно.

Для проверки работы сервера DNS с помощью DIG выполните следующие действия:

1. Введите в командной строке DIG HOSTNAME('127.0.0.1') REVERSE(*YES).

   Должна быть показана следующая информация, содержащая имя хоста с циклическим адресом:

```
;; глобальные опции: printcmd
;; Получен ответ:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id:865
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL:1

;; QUESTION SECTION:
;1.0.0.127.in-addr.arpa.          IN   PTR

;; ANSWER SECTION:
1.0.0.127.in-addr.arpa.  86400   IN    PTR  localhost.

;; AUTHORITY SECTION:
0.0.127.in-addr.arpa.   86400   IN    NS   ISA2LP05.RCHLAND.IBM.COM.

;; ADDITIONAL SECTION:
ISA2LP05.RCHLAND.IBM.COM. 38694   IN    A   9.5.176.194
```

```
;; Query time: 552 msec
;; SERVER: 9.5.176.194#53(9.5.176.194)
;; WHEN: Thu May 31 21:38:12 2007
;; MSG SIZE rcvd: 117
```

Правильный ответ сервера должен содержать имя **localhost** в качестве имени хоста с циклическим адресом.

2. Для выхода из сеанса нажмите Enter.

Примечание: Для получения справки по команде DIG введите `?DIG` и нажмите Enter.

Управление ключами защиты

Вы можете ограничить доступ к данным DNS с помощью ключей защиты.

В службе DNS применяются ключи двух типов: ключи DNS и ключи динамического обновления. Каждый из них играет свою роль для защиты конфигурации сервера DNS. Ниже приведена информация о применении этих ключей для защиты сервера DNS.

Управление ключами DNS

Управление ключами DNS применяется сервером DNS при проверке запросов на обновление информации.

Вы можете задать ключ и присвоить ему имя. Для того чтобы настроить защиту объекта DNS, например динамической области, укажите этот ключ в Списке адресов для сравнения.

Для работы с ключами DNS выполните следующие действия:

1. В System i Navigator, разверните список ***ваша система*** → **Сеть** → **Серверы** → **DNS**.
2. В правой панели щелкните правой кнопкой мыши на имени экземпляра сервера DNS и выберите пункт **Конфигурация**.
3. В окне Конфигурация DNS выберите **Файл** → **Управление ключами**.

В окне Управление ключами можно выполнить требуемые задачи.

Управление ключами для динамического обновления

Ключи для динамического обновления применяются сервером DHCP, выполняющим динамическое обновление информации об области.

Эти ключи используются, когда серверы DNS и DHCP установлены в одной системе System i. Если DHCP находится в другой системе System i, вам потребуется расположить одни и те же файлы ключей динамического обновления в каждой удаленной системе System i, которой они необходимы для отправки динамических обновлений на ответственные серверы. Эти файлы можно распространять с помощью FTP, электронной почты и так далее.

Для работы с ключами для динамического обновления выполните следующие действия:

1. В System i Navigator, разверните список ***ваша система*** → **Сеть** → **Серверы** → **DNS**.
2. Щелкните правой кнопкой мыши на пункте **DNS** и выберите опцию **Работа с ключами для динамического обновления**.

После этого в окне Управление ключами динамического обновления можно выполнить соответствующие задачи.

Просмотр статистики сервера DNS

Для получения информации о работе сервера и его производительности создайте дамп базы данных или воспользуйтесь средствами сбора статистики.

Сервер DNS предоставляет несколько средств диагностики. С их помощью можно получить информацию о работе сервера.

Ссылки, связанные с данной

“Работа с файлами конфигурации DNS” на стр. 35
Для создания экземпляров сервера DNS в системе System i и работы с ними применяется служба DNS i5/OS. Функции для работы с файлами конфигурации DNS предусмотрены в Навигаторе System i NavigatorSystem i Navigator

Просмотр статистики сервера DNS

Статистическая информация содержит итоговое число запросов и ответов, полученных сервером с момента его запуска или загрузки его базы данных.

Служба DNS позволяет получить статистическую информацию о работе экземпляра сервера. Файл статистики непрерывно пополняется. С помощью этой информации можно получить представление о нагрузке на сервер и найти причину ошибки. Дополнительная информация о статистике работы сервера приведена в разделе Статистическая информация о сервере DNS электронной справки по серверу DNS.

Для просмотра статистической информации о работе сервера выполните следующие действия:

1. В System i Navigator, разверните список ***ваша система*** → **Сеть** → **Серверы** → **DNS**.
2. В правой панели щелкните правой кнопкой мыши на ***значке сервера DNS*** и выберите пункт **Конфигурация**.
3. В окне Конфигурация DNS выберите **Показать** → **Статистика сервера**.

Для просмотра статистической информации сервера, которая хранится в файле named.stats, можно также использовать команду Удаленное управление демоном имен (RNDC).Она применяется следующим образом.

```
RNDC RNDCCMD('stats')
```

Просмотр базы данных активного сервера

База данных активного сервера содержит информацию об области и хосте, в том числе некоторые свойства области (например, начало области ответственности (SOA)) и хоста (например, система обмена почтой (MX)).

Служба DNS позволяет просмотреть дамп области ответственности, кэша и подсказок экземпляра сервера. Такой дамп содержит информацию обо всех основных и вспомогательных областях прямого и обратного преобразования, а также сведения, полученные сервером из ответов на запросы.

Дамп базы данных активного сервера можно просмотреть с помощью System i Navigator. Если вам необходимо сохранить копии файлов, то файл дампа базы данных с именем named_dump.db будет располагаться в каталоге i5/OS: `/QIBM/UserData/OS400/DNS/<экземпляр сервера>/`, где *<экземпляр сервера>* - это имя экземпляра сервера DNS. За дополнительной информацией о базе данных активного сервера обратитесь к разделу Дамп базы данных сервера DNS электронной справки по серверу DNS.

Для просмотра дампа базы данных активного сервера выполните следующие действия:

1. В System i Navigator, разверните список ***ваша система*** → **Сеть** → **Серверы** → **DNS**.
2. В правой панели щелкните правой кнопкой мыши на ***значке сервера DNS*** и выберите пункт **Конфигурация**.
3. В окне Конфигурация DNS выберите **Показать** → **База данных активного сервера**.

Для просмотра информации файла named_dump.db можно использовать также команду Удаленное управление демоном имен (RNDC). Она применяется следующим образом.

```
RNDC RNDCCMD('dumpdb -all')
```

Работа с файлами конфигурации DNS

Для создания экземпляров сервера DNS в системе System i и работы с ними применяется служба DNS i5/OS. Функции для работы с файлами конфигурации DNS предусмотрены в Навигаторе System i NavigatorSystem i Navigator

Ниже перечислены каталоги интегрированной файловой системы, в которой хранятся файлы конфигурации DNS.

Примечание: Показанная ниже файловая структура относится к DNS с поддержкой BIND 9.

В приведенной ниже таблице описана иерархия каталогов, в которых расположены файлы конфигурации. Файлы, отмеченные значком  , необходимо регулярно сохранять для защиты данных. Файлы, отмеченные значком  , необходимо регулярно удалять.

Имя	Значок	Описание
/QIBM/UserData/OS400/DNS/		Начальный каталог DNS.
/QIBM/UserData/OS400/DNS/ <*экземпляр-n*>/		Начальный каталог для экземпляра сервера.
ATTRIBUTES		С помощью этого файла сервер DNS определяет поддерживаемую версию BIND.
BOOT.AS400BIND4		Этот файл содержит параметры конфигурации и стратегии сервера BIND 4.9.3. На его основе был создан файл named.conf для данного экземпляра сервера, поддерживающего BIND 8. Этот файл создается при переходе от сервера BIND 4.9.3 к серверу BIND 9. Он служит резервной копией старой конфигурации, к которой при необходимости можно вернуться. После того как вы проверите правильность работы сервера BIND 9, этот файл можно удалить.
named.ca		Список корневых серверов для данного экземпляра сервера.
named.conf		Этот файл содержит информацию о конфигурации. В нем перечислены области, за которые отвечает сервер, задано расположение файлов с информацией об областях, указаны области, для которых разрешено динамическое обновление, адреса серверов пересылки и другие параметры.
named_dump.db		Дамп базы данных активного сервера.
named.memstats		Статистические данные об использовании памяти на сервере (если опция настроена в файле named.conf).

Имя	Значок	Описание
named.pid		В этом файле хранится ИД процесса, связанный с активным сервером. Этот файл создается при каждом запуске сервера DNS. Он необходим для работы таких функций сервера, как База данных, Статистика и Обновить сервер. Не удаляйте и не изменяйте этот файл.
named.random		Файл со случайными данными, созданный сервером.
named.recursing		Запросы серверов, которые являются рекурсивными (при соответствующем запросе System i Navigator).
named.run		Протокол отладки по умолчанию (если запрошен). Такие файлы могут существовать под именами named.run.0, named.run.1 и так далее.
named.stats		Статистическая информация о сервере.
<*основная-область-n*>.db		Это файл основной области для отдельного домена на этом сервере. Этот файл содержит все записи о ресурсах, относящиеся к области. Для каждой области создается отдельный файл .db.
<*основная-область-n*>.jnl		Файл журнала, который содержит динамические обновления области. Он создается при получении первого динамического обновления. При перезапуске сервера после завершения работы или сбоя системы он воспроизводит действия, зарегистрированные в файле журнала, для применения всех обновлений области, которые происходили после создания последнего дампа области. Также этот файл используется для передачи измененной информации об области (IXFR). Эти файлы журналов не удаляются. Они являются двоичными, и их не следует редактировать.
db.<*вспомогательная-область-n*>		Это файл вспомогательной области для отдельного домена на этом сервере. Этот файл содержит все записи о ресурсах, относящиеся к области. Он используется для начальной загрузки вспомогательного сервера при запуске, если основной сервер недоступен. Для каждой области создается отдельный файл .db.
/QIBM/UserData/OS400/DNS/_DYN/		Этот каталог содержит файлы, необходимые для динамического обновления данных.

Имя	Значок	Описание
<*ид-ключа-n*>._KEY		.Symlink к ключу DNSSEC с ключом <*ид-ключа-n*>. Всегда указывает на последний созданный ключ K<*ид-ключа-n*>.+*ааа*+*nnnnn*.key.
<*ид-ключа-x*>._DUK. <*область-a*>		Ключ, необходимый для динамического обновления информации об <*области-a*> с помощью ключа с именем <*ид-ключа-x*>.
<*ид-ключа-x*>._KID		Этот файл содержит оператор для ключа с ид-ключа <*ид-ключа-y*>.
<*ид-ключа-y*>._DUK. <*область-a*>		Ключ, необходимый для динамического обновления информации об <*области-a*> с помощью ключа с именем <*ид-ключа-y*>.
<*ид-ключа-y*>._DUK. <*область-b*>		Ключ, необходимый для динамического обновления информации об <*области-b*> с помощью ключа с именем <*ид-ключа-y*>.
<*ид-ключа-y*>._KID		Этот файл содержит оператор для ключа с ид-ключа <*ид-ключа-y*>.
rndc-confgen.random.*nnnnnn*		Файлы со случайными данными для различных команд, которым они необходимы. Часть *nnnnn* означает номер задания, которое создало файл. Они остаются только если команда по какой-либо причине прекращает выполняться и не удаляет их.

Понятия, связанные с данным

“Определение прав доступа для работы с DNS” на стр. 24
Администратору сервера DNS должны быть предоставлены особые права доступа. Следует тщательно продумать, какие именно права доступа можно предоставить администратору без ущерба для защиты сервера.

“Просмотр статистики сервера DNS” на стр. 33
Для получения информации о работе сервера и его производительности создайте дамп базы данных или воспользуйтесь средствами сбора статистики.

Задачи, связанные с данной

“Настройка серверов имен” на стр. 28
Вы можете создать несколько экземпляров серверов имен. В этом разделе приведены инструкции по настройке сервера имен.

Дополнительные функции DNS

В этом разделе описаны дополнительные функции, которые системные администраторы могут применять для более эффективного управления сервером DNS.

В программе System i Navigator предусмотрен интерфейс с дополнительными функциями для настройки сервера DNS и работы с ним. Ниже приведена краткая информация о выполнении некоторых процедур, предназначенная для тех администраторов, кто уже знаком с графическим интерфейсом для работы с системой i5/OS. В частности, здесь описаны эффективные способы изменения состояния и атрибутов сразу нескольких экземпляров серверов.

Задачи, связанные с данной

“Изменение параметров отладки сервера DNS” на стр. 41
Функция отладки сервера DNS позволяет получить информацию, полезную для обнаружения и устранения неполадок сервера DNS.

Запуск и завершение работы серверов DNS

Если Система имен доменов (DNS) в интерфейсе System i Navigator не позволяет одновременно запускать несколько экземпляров сервера или завершать их работу, то для одновременного изменения этих установок для нескольких экземпляров можно использовать текстовый интерфейс.

Для того чтобы запустить все экземпляры сервера DNS, введите команду `STRTCPSVR SERVER(*DNS) DNSSVR(*ALL)`.Для того чтобы остановить все экземпляры сервера DNS, введите команду `ENDTCPSVR SERVER(*DNS) DNSSVR(*ALL)`.

Изменение уровня отладки

Изменение уровня отладки может применяться в том случае, когда информация об области занимает большой объем памяти, и администратор хочет избежать создания излишней отладочной информации при загрузке данных области во время запуска сервера.

Интерфейс для работы с DNS, предусмотренный в System i Navigator, не позволяет изменить уровень отладки для активного сервера. Эту задачу можно выполнить с помощью текстового интерфейса. Для того чтобы изменить уровень отладки с помощью текстового интерфейса, выполните описанные ниже действия, заменив в команде выражение *nnnnn* на имя экземпляра сервера:

1. Введите `ADDLIBLE QDNS` в командной строке и нажмите Enter.
2. Измените уровень отладки:
   - Для включения отладки или увеличения уровня отладки на 1 введите `RNDC RNDCCMD('trace')` и нажмите клавишу Enter.
   - Для выключения отладки введите команду `RNDC RNDCCMD('notrace')` и нажмите клавишу Enter.

Устранение неполадок в Системе имен доменов

Параметры ведения протокола и отладки сервера DNS помогут вам устранить неполадки в работе сервера DNS.

Принцип работы DNS мало отличается от других функций и приложений TCP/IP. Подобно приложениям SMTP и FTP, задания DNS выполняются в подсистеме QSYSWRK и создают протоколы от имени пользовательского профайла QTCP. С помощью протокола вы можете определить причину завершения работы задания DNS. Если сервер DNS отправляет неверные ответы на запросы, то с помощью протоколов задания вы можете определить причину ошибки.

Информация о конфигурации DNS хранится в нескольких файлах, каждый из которых содержит записи определенного типа. Чаще всего неполадки в работе сервера DNS связаны с ошибками в записях, хранящихся в файлах конфигурации. При возникновении неполадки в первую очередь проверьте правильность этих записей.

Наименование заданий

Если вы решили просмотреть протокол задания (например, с помощью команды WRKACTJOB) и убедиться в правильности работы сервера DNS, обратите внимание на следующие правила именования заданий:

- Если в системе настроены серверы, основанные на стандарте BIND 9, то для каждого из них будет создано отдельное задание. Имена заданий начинаются с префикса QTOBD, за которым следует имя экземпляра сервера. Например, если в системе создано два экземпляра сервера, INST1 и INST2, то для них будут запущены задания QTOBDINST1 и QTOBDINST2.

Регистрация сообщений сервера DNS

Служба DNS предоставляет несколько параметров ведения протокола, которые можно изменить для обнаружения причины неполадки. Вы можете настроить эти параметры для получения интересующей вас информации о неполадках, выбрав уровень серьезности, категории сообщений и файлы вывода.

В стандарте BIND 9 предусмотрено несколько параметров ведения протокола. Теперь вы можете выбрать типы сообщений, которые должны заноситься в протокол; протокол, в который должны заноситься сообщения определенного типа; а также уровень серьезности сообщений, которые должны заноситься в протокол. В общем случае рекомендуется оставить для параметров ведения протокола значения по умолчанию. Если вы решите изменить эти значения, предварительно ознакомьтесь с другими источниками информации о стандарте BIND 9.

Каналы для записи сообщений

Сервер DNS может записывать сообщения в различные каналы вывода. Канал вывода определяет объект, в котором сохраняются сообщения. Существуют каналы вывода следующих типов:

- **Каналы типа файл**

  При записи сообщения в такой канал оно сохраняется в файле. По умолчанию применяются два канала типа Файл: i5os_debug и i5os_QPRINT. В канал i5os_debug записываются отладочные сообщения. Этот канал соответствует файлу named.run. Вы можете выбрать и другие категории сообщений, которые должны записываться в этот канал. Сообщения из канала i5os_QPRINT записываются в буферный файл QPRINT, связанный с пользовательским профайлом QTCP. В дополнение к каналам по умолчанию вы можете создать собственные каналы типа Файл.

- **Системный протокол**

  Сообщения из этого канала записываются в протокол задания сервера. По умолчанию применяется канал i5os_joblog. Сообщения из этого канала записываются в протокол задания экземпляра сервера DNS.

- **Фиктивный канал**

  Сообщения, заносимые в этот канал, удаляются. По умолчанию применяется фиктивный канал i5os_null. В этот канал следует направлять все сообщения, которые не нужно записывать ни в один протокол.

Категории сообщений

Все сообщения разбиты на несколько категорий. Вы можете выбрать категории сообщений, которые будут заноситься в каждый канал записи сообщений. Можно выбрать такие категории:

клиент Обработка запросов клиентов.

config Анализ и обработка файла конфигурации.

база данных
Сообщения, относящиеся к базам данных, которые предназначены для внутреннего использования сервером DNS для хранения данных областей и кэша.

по умолчанию
Определение опций регистрации для категорий, для которых не определена специфическая конфигурация.

delegation-only
Только делегирование. Регистрирует запросы, возвратившие значение NXDOMAIN по причине того, что в определении области, области подсказок или ограниченной области указан атрибут delegation-only.

dispatch
Диспетчеризация входящих пакетов на модули сервера, которые будут их обрабатывать.

dnssec Обработка протоколов Расширений защиты DNS (DNSSEC) и Подписи транзакции (TSIG).

general
Общая категория, используемая для элементов, которые не были отнесены ни к какой другой категории.

lame-servers
Неисправные серверы, в настройках которых присутствуют ошибки, найденные BIND 9 при попытке отправки запроса к этим серверам во время преобразования.

сеть Сетевые операции.

notify Протокол NOTIFY.

resolver
Преобразование DNS, например, рекурсивный поиск, который производится от имени клиентов кэширующим сервером имен.

security
Утверждение и отклонение запросов.

xfer-in Принимаемая сервером передача информации об области.

xfer-out
Отправляемая сервером передача информации об области.

unmatched
Сообщения, для которых не удалось определить класс или для которых отсутствует соответствующее представление. Резюме, состоящее из одной строки, регистрируется также в категории клиент. Лучше всего выводить эту категорию в файл или stderr. По умолчанию она направляется в нулевой канал.

update Динамические обновления.

update-security
Утверждение и отклонение запросов на обновление. В запросах определяется, следует ли их регистрировать. При запуске указание запросов по категориям позволяет регистрировать запросы даже если не указана опция querylog.

В записи о запросе указывается IP-адрес клиента и номер порта, а также имя, класс и тип запроса. Кроме того, в нем определяется, установлен ли флаг Требуется рекурсия (+ установлен, - нет), использовалась ли EDNS (E) и был ли запрос подписан (S).

Если вы не будете регулярно удалять файлы протоколов, то они могут достигнуть очень больших размеров. При запуске и остановке сервера DNS все файлы протоколов очищаются.

Уровень серьезности сообщений

Сообщения, заносимые в канал, могут отфильтровываться в зависимости от их уровня серьезности. Для каждого канала можно задать уровень серьезности сообщений, которые должны записываться в этот канал. Существуют следующие уровни серьезности сообщений:

- Критическая ситуация
- Ошибка
- Предупреждение
- Извещение
- Информация
- Отладка (укажите уровень отладки от 0 до 11)
- Динамический (соответствует уровню отладки, который устанавливается при запуске сервера)

В канал заносятся все сообщения, уровень серьезности которых не ниже указанного. Например, если вы выберете уровень серьезности Предупреждение, то в канал будут записываться сообщения с уровнем серьезности Предупреждение, Ошибка и Критическая ситуация. Если вы выберете уровень серьезности

Отладка, укажите уровень отладки от 0 до 11, сообщения для которого должны записываться в канал.

Изменение параметров регистрации

Для изменения параметров ведения протокола выполните следующие действия:

1. В System i Navigator, разверните список ***ваша система*** → **Сеть** → **Серверы** → **DNS**.
2. В правой панели щелкните правой кнопкой мыши на ***значке сервера DNS*** и выберите пункт **Конфигурация**.
3. В окне Конфигурация сервера DNS щелкните правой кнопкой мыши на **значке сервера DNS** и выберите пункт **Свойства**.
4. В окне Свойства сервера щелкните на вкладке **Каналы**, чтобы создать новые каналы типа Файл или задать свойства канала, например, уровень серьезности сообщений, записываемых в канал.
5. В окне Свойства сервера щелкните на вкладке **Ведение протокола** и выберите категории сообщений, которые должны заноситься в тот или иной канал.

Совет по устранению неполадок при работе с уровнями серьезности

Для канала i5os_joblog по умолчанию установлен уровень серьезности Ошибка. При этом в протокол не заносятся информационные сообщения и предупреждения, которые могут значительно увеличить размер протокола, что может отрицательно сказаться на производительности системы. Если в системе возникла неполадка, однако в протоколе задания не указана причина этой неполадки, то рекомендуется изменить уровень серьезности. Для этого перейдите на страницу Каналы, следуя приведенным выше инструкциям, и измените для канала i5os_joblog уровень серьезности на Предупреждение, Извещение или Информация. После устранения неполадки восстановите прежний уровень серьезности, для того чтобы сократить число сообщений, заносимых в протокол задания.

Изменение параметров отладки сервера DNS

Функция отладки сервера DNS позволяет получить информацию, полезную для обнаружения и устранения неполадок сервера DNS.

DNS поддерживает 12 уровней отладки. Обычно для обнаружения неполадок создается протокол сообщений, однако в некоторых случаях требуется включить отладку. Обычно отладка выключена (уровень отладки = 0). Перед включением этой функции попытайтесь определить причину неполадки с помощью протокола.

Сервер поддерживает уровни отладки от 0 до 11. Выбрать правильный уровень отладки для диагностики возникшей неполадки вам помогут в сервисном представительстве фирмы IBM. Если уровень отладки отличен от нуля, то сервер записывает отладочную информацию в файл named.run, расположенный в следующем каталоге системы i5/OS: `/QIBM/UserData/OS400/DNS/<экземпляр сервера>`, где *<экземпляр сервера>* - имя экземпляра сервера DNS. Во время работы сервера DNS с ненулевым уровнем отладки размер файла named.run постоянно увеличивается. На странице Свойства сервера - Каналы можно задать максимальный размер и число версий файла named.run.

Для того чтобы изменить уровень отладки для экземпляра сервера DNS, выполните следующие действия:

1. В System i Navigator, разверните список ***ваша система*** → **Сеть** → **Серверы** → **DNS**.
2. В правой панели щелкните правой кнопкой мыши на ***значке сервера DNS*** и выберите пункт **Конфигурация**.
3. В окне Конфигурация сервера DNS щелкните правой кнопкой мыши на имени сервера DNS и выберите пункт **Свойства**.
4. На странице Свойства сервера - Общие укажите начальный уровень отладки сервера.
5. Если сервер активен, перезапустите его.

Примечание: Изменение уровня отладки вступает в силу только после перезапуска сервера. Указанный на этой странице уровень отладки устанавливается только при запуске сервера. Информация о том, как изменить уровень отладки активного сервера, приведена в разделе Дополнительные функции DNS.

Понятия, связанные с данным

“Дополнительные функции DNS” на стр. 37
В этом разделе описаны дополнительные функции, которые системные администраторы могут применять для более эффективного управления сервером DNS.

Связанная информация по DNS

Публикации IBM Redbooks, Web-сайты и другие разделы information center содержат информацию, которая связана с разделами о Системе имен доменов. Документы в формате PDF можно просмотреть или распечатать.

IBM Redbooks

AS/400 TCP/IP Autoconfiguration: DNS and DHCP Support  (5181 Кб)

В этом руководстве Redbooks описаны серверы DNS и DHCP в операционной системе i5/OS. В нем на примерах показаны процедуры установки, настройки устранения неполадок служб DNS и DHCP.

Web-сайты

- *DNS and BIND*, fifth edition. Paul Albitz and Cricket Liu. Издательство O’Reilly and Associates,Inc.  Sebastopol, California, 2006. ISBN: 0-59610-057-4.
- Справочное руководство администратора BIND (в формате PDF) с Web-сайта Internet System Consortium (ISC)  .
- Web-сайт Internet Software Consortium  содержит новости, ссылки на другие источники информации и прочие ресурсы по BIND.
- Web-сайт InterNIC  содержит каталог зарегистрированных имен доменов, утвержденных организацией ICANN.
- DNS Resources Directory  содержит справочные материалы по DNS и ссылки на многие другие ресурсы, в том числе на конференции по DNS. Кроме того, здесь можно найти список RFC, относящихся к DNS  .

Ссылки, связанные с данной

“Документ в формате PDF о Системе имен доменов” на стр. 2
Можно просмотреть и распечатать файл PDF с данной информацией.

Приложение. Примечания

Настоящая документация была разработана для продуктов и услуг, предлагаемых на территории США.

IBM может не предлагать продукты и услуги, упомянутые в этом документе, в других странах. Информацию о продуктах и услугах, предоставляемых в вашей стране, вы можете получить в местном представительстве IBM. Ссылки на продукты, программы или услуги IBM не означают, что можно использовать только указанные продукты, программы или услуги IBM. Вместо них можно использовать любые другие функционально эквивалентные продукты, программы или услуги, не нарушающие прав IBM на интеллектуальную собственность. Однако в этом случае ответственность за проверку работы этих продуктов, программ и услуг возлагается на пользователя.

IBM могут принадлежать патенты или заявки на их получение, относящиеся к материалам этого документа. Предоставление вам настоящего документа не означает предоставления каких-либо лицензий на эти патенты. Запросы на приобретение лицензий можно отправлять по следующему адресу:

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785
U.S.A.

Запросы на лицензии, связанные с информацией DBCS, следует направлять в отдел интеллектуальной собственности в местном представительстве IBM или в письменном виде по следующему адресу:

IBM World Trade Asia Corporation
Licensing
2-31 Roppongi 3-chome, Minato-ku
Tokyo 106-0032, Japan

Следующий абзац не относится к Великобритании, а также к другим странам, в которых это заявление противоречит местному законодательству: INTERNATIONAL BUSINESS MACHINES CORPORATION ПРЕДОСТАВЛЯЕТ НАСТОЯЩУЮ ПУБЛИКАЦИЮ НА УСЛОВИЯХ “КАК ЕСТЬ”, БЕЗ КАКИХ-ЛИБО ЯВНЫХ ИЛИ ПОДРАЗУМЕВАЕМЫХ ГАРАНТИЙ, ВКЛЮЧАЯ, НО НЕ ОГРАНИЧИВАЯСЬ ЭТИМ, НЕЯВНЫЕ ГАРАНТИИ СОБЛЮДЕНИЯ ПРАВ, КОММЕРЧЕСКОЙ ЦЕННОСТИ И ПРИГОДНОСТИ ДЛЯ КАКОЙ-ЛИБО ЦЕЛИ. В некоторых странах запрещается отказ от каких-либо явных и подразумеваемых гарантий при заключении определенных договоров, поэтому данное заявление может не действовать в вашем случае.

В данной публикации могут встретиться технические неточности и типографские опечатки. В информацию периодически вносятся изменения, которые будут учтены во всех последующих изданиях настоящей публикации. Компания IBM может вносить изменения в продукты и программы, описанные в этой публикации в любое время без предварительного уведомления.

Все встречающиеся в данной документации ссылки на Web-сайты других компаний предоставлены исключительно для удобства пользователей и не являются рекламой этих Web-сайтов. Материалы, размещенные на этих Web-сайтах, не являются частью информации по данному продукту IBM и ответственность за применение этих материалов лежит на пользователе.

IBM может использовать и распространять любую предоставленную вами информацию на свое усмотрение без каких-либо обязательств перед вами.

© Copyright IBM Corp. 1998, 2008

Для получения информации об этой программе для обеспечения: (i) обмена информацией между независимо созданными программами и другими программами (включая данную) и (ii) взаимного использования информации, полученной в ходе обмена, пользователи данной программы могут обращаться по адресу:

IBM
Corporation
Software Interoperability Coordinator, Department YBWA
3605 Highway 52 N
Rochester, MN 55901
U.S.A.

Такая информация может предоставляться на определенных условиях, включая, в некоторых случаях, уплату вознаграждения.

Описанная в этом документе лицензионная программа и все связанные с ней лицензионные материалы предоставляются IBM в соответствии с условиями Соглашения с заказчиком IBM, Международного соглашения о лицензии на программу IBM Лицензионного соглашения на машинный код IBM или любого другого эквивалентного соглашения.

Все приведенные показатели производительности были получены в управляемой среде. В связи с этим результаты, полученные в реальной среде, могут существенно отличаться от приведенных. Некоторые измерения могли быть выполнены в системах, находящихся на этапе разработки, поэтому результаты измерений, полученные в серийных системах, могут отличаться от приведенных. Более того, некоторые значения могли быть получены в результате экстраполяции. Реальные результаты могут отличаться от указанных. Пользователи, работающие с этим документом, должны удостовериться, что используемые ими данные применимы в имеющейся среде.

Информация о продуктах других изготовителей получена от поставщиков этих продуктов, из их официальных сообщений и других общедоступных источников. IBM не выполняла тестирование этих продуктов других фирм и не может подтвердить точность заявленной информации об их производительности, совместимости и других свойствах. Запросы на получение дополнительной информации об этих продуктах должны направляться их поставщикам.

Все заявления, касающиеся намерений и планов IBM, могут изменяться и отзываться без предварительного уведомления, и отражают только текущие цели и задачи.

Эта информация содержит примеры данных и отчетов, применяемых в повседневной работе. Для того чтобы примеры были максимально наглядными, в них указаны имена людей, а также названия компаний, товарных знаков и продуктов. Все они являются вымышленными, и любое совпадение с реально существующими именами и названиями случайно.

Лицензия на продукты, защищенные авторским правом:

Эта информация содержит примеры приложений на исходном языке, иллюстрирующие приемы программирования в различных операционных платформах. Разрешается бесплатно копировать, изменять и распространять эти примеры кода в любом виде с целью разработки, использования, рекламирования или распространения приложений, отвечающих требованиям интерфейса операционной платформы, для которой предназначены эти примеры кода. Работа примеров не была проверена во всех возможных условиях. По этой причине IBM не может прямо или косвенно гарантировать правильность их работы, надежность и возможность обслуживания.

Любая копия или часть этих примеров программ, а также произведений, созданных на их основе, должна содержать следующее заявление об авторских правах:

© (название вашей фирмы) (год). Части этого кода были созданы на основе примеров программ IBM Corp. Corp. © Copyright IBM Corp. _год или годы_. Все права защищены.

В электронной версии данной документации фотографии и цветные иллюстрации могут отсутствовать.

Сведения о программных интерфейсах

Данная публикация о системе имен доменов (DNS) включает в себя документацию по программным интерфейсам, позволяющим заказчику писать программы для получения доступа к службам IBM i5/OS.

Товарные знаки

Ниже перечислены товарные знаки International Business Machines Corporation в США и/или других странах:

AS/400 i5/OS
IBM IBM (эмблема)
OS/400 Справочники
System i

Adobe, логотип Adobe, PostScript и логотип PostScript являются зарегистрированными товарными знаками или товарными знаками Adobe Systems Incorporated в Соединенных штатах Америки и/или в других странах.

Другие названия фирм, продуктов и услуг могут являться товарными знаками или знаками обслуживания других фирм.

Условия и соглашения

Разрешение на использование этих публикаций предоставляется в соответствии с следующими условиями и соглашениями.

Личное использование: Вы можете воспроизводить эти публикации для личного, некоммерческого использования при условии сохранения информации об авторских правах. Данные публикации, а также любую их часть запрещается распространять, демонстрировать или использовать для создания других продуктов без явного согласия IBM.

Коммерческое использование: Вы можете воспроизводить, распространять и демонстрировать эти публикации в рамках своей организации при условии сохранения информации об авторских правах. Данные публикации, а также любую их часть запрещается воспроизводить, распространять, использовать для создания других продуктов и демонстрировать вне вашей организации, без явного согласия IBM.

На данные публикации, а также на содержащиеся в них сведения, данные, программное обеспечение и другую интеллектуальную собственность, не распространяются никакие другие разрешения, лицензии и права, как явные, так и подразумеваемые, кроме оговоренных в настоящем документе.

IBM сохраняет за собой право аннулировать предоставленные настоящим документом разрешения в том случае, если по мнению IBM использование этих публикаций может принести ущерб интересам IBM или если IBM будет установлено, что приведенные выше инструкции не соблюдаются.

Вы можете загружать, экспортировать и реэкспортировать эту информацию только в полном соответствии со всеми применимыми законами и правилами, включая все законы США в отношении экспорта.

IBM не несет ответственности за содержание этих публикаций. Публикации предоставляются на условиях ″как есть″, без предоставления каких-либо явных или подразумеваемых гарантий, включая, но не ограничиваясь этим, подразумеваемые гарантии коммерческой ценности, отсутствия нарушений или применения для каких-либо конкретных целей.

Напечатано в Дании