Практическая работа к занятию №7

DNS

Цель работы: закрепить понимание принципов работы DNS, получить практические навыки использования утилит работы с серверами системы DNS и конфигурирования DNS сервера на платформе Linux;

Требования: установленная на компьютере среда виртуализации ORACLE Virtual Box с виртуальной машиной Linux Cent OS 7 (выполнять работу можно в любой ОС Linux, но все описания будут даваться для CentOS 7).

Краткие теоретические сведения

Система DNS – распределенная база данных, хранящая соответствие между IP адресом и доменным именем компьютера. Система DNS – клиент - серверная. DNS-клиент получает в качестве конфигурационного параметра IP адрес обслуживающего DNS-сервера и получает к нему доступ напрямую.

DNS сервер может хранить данные о одном или нескольких доменах или просто обрадовать клиентские запросы по разрешению имени.

Существуют множество типов ресурсных записей:

a. SOA (Start of Authority/начальная запись зоны) - конфигурационная запись домена, управляющая кэшированием и синхронизацией копии зоны,
b. A — (address record/запись адреса) - запись адреса в протоколе IPv4,
c. AAAA (IPv6 address record) аналогична записи A, но для IPv6,
d. CNAME (canonical name record/каноническая запись имени (псевдоним)), например WWW,
e. MX (mail exchange) – конфигурация почтовых серверов,
f. NS (name server/сервер имён) – записи о доменных серверов в доменах,
g. PTR (pointer) – указатели на DNS имена в зонах обратного просмотра,
h. SRV (server selection) – записи, указывающие на службы, например LDAP
i. TXT – текстовые записи, например SPF и DKIM, которые защищают от подделки домена при отправке писем

Для платформы Linux самым распространенным и исторически старым является сервер BIND.

Конфигурационные файлы сервера находятся в каталоге /etc/ и /etc/named.

Утилиты, позволяющие делать клиентские запросы к системе DNS входят в пакет bind-utils. К нгим относится утилита dig.

На Linux CentOS7 для установки пакетов служит утилита yum.

Для управления запуском и просмотра состояния сервиса используется системная утилита systemctl.

Добавить разрешение службе работать через локальный firewall можно с помощью утилиты firewall-cmd

Подробная информация о bind - https://bind9.readthedocs.io/en/v9_16_6/reference.html#

Инструментальные средства:

Утилиты: firewall-cmd systemctl ip ping journalctl ss netstat lsof dig

Файлы:	/etc/named.conf, /etc/named
Утилиты работы с текстом:	echo, grep, sed
Редакторы:	vi, nano

Порядок выполнения работы

Далее описан порядок выполнения работы. Пункты работы, результаты которых прямо или косвенно используются в отчете, помечены знаком **(!)**.

Часть 1. Подготовка и проверка конфигурации.

В VirtualBox:

1. Сделайте связанный клон виртуальной машины. Одну машину назовите c7-1, другой c7-2
2. Для виртуальной машины c7-1 добавьте второй сетевой интерфейс.
3. Подключите сетевой интерфейс c7-2 и новый сетевой интерфейс c7-1 к внутренней сети intnet.
4. Подключите исходный сетевой интерфейс c7-1 к NAT.

В Linux :

5. Для внутренней сети задайте для машин c7-1 и c7-2 адреса 10.0.0.1 и 10.0.0.2 с маской 255.255.255.0.
6. Для исходного интерфейса c7-1 оставьте получение адреса автоматически от dhcp сервара VirtualBox
7. Для обоих хостов отключите использование ipv6.
8. Задайте имена хостов, советующие именам виртуальных машин.
9. Проверьте доступность хостов по внутренней сети и доступность внешней сети на хосте c7-1.
10. Убедитесь, что на c7-2 в качестве шлюза по умолчанию и DNS задан адрес c7-1.
11. Установите на машине c7-1 пакеты bind и bind-utils

Часть 2. Получение информации из DNS с помощью утилиты dig

1. На хосте c7-1 с выполните команду dig www.itmo.ru. В консольном выводе изучите состав секций HEADER, QUESTION SECTION, ANSWER SECTION, AUTHORITY SECTION, SERVER: 192.168.0.1, WHEN и MSG SIZE. Соотнесите значения полей секции HEADER со значениями остальных полей. **(!)**

2. На хосте c7-1 с помощью утилиты dig решите следующие задачи **(!)**:
    a. Выведите только результат разрешения имени www.itmo.ru (только IP адрес),
    b. Выведите на экран подробную информацию о разрешении имени, с выводом всех промежуточных серверов, определите какой именно DNS сервер вернул IP адрес хоста.
    c. Выведите конфигурационную запись (SOA) домена itmo.ru, определите, значения каждого из числовых параметров записи, что они означают?
    d. Определите, какие сервера обрабатывают почту домена itmo.ru.
    e. Определите какие DNS сервера обслуживают зону itmo.ru и какие у них ip адреса.

f. Значение записи в зоне обратного просмотра для 87.250.250.242.
g. Определите количество серверов, поддерживающих корневую зону.

Часть 3. Настройка кэширующего DNS сервера

Цель этой части – настроить хост c7-1 как кэширующий DNS сервер для хоста c7-2.

1. С помощью утилиты firewall-cmd разрешите службе dns получать доступ к сети.
2. С помощью systemctl включите и запустите службу bind (она называется named)
3. Отредактируйте /etc/named.conf так, чтобы:
    a. Сервер отвечал на IPv4 адресе из вашей локальной сети,
    b. Не работал поверх IPv6
    c. Позволял обычные и рекурсивные запросы только с ip адресов вашей локальной сети (между c7-1 и c7-2) и с самого хоста c7-1.
    d. Делал рекурсивные запросы.
    e. Вместо версии сервера выводил при запросе «My Own DNS Server»
4. Проверьте разрешение имен на хосте c7-2.

Часть 4. Создание собственной доменной зоны

1. Отредактируйте /etc/named.conf так, чтобы добавить зону на сервер зону домена <fio>.local, где <fio> - ваши инициалы, причем ваш сервер должен быть для этого домена основным, не допускать трансфер зоны, разрешать все обновления и хранить зону в файле /var/named/<fio>.local.db
2. Для проверки файла конфигурации используйте утилиту named-checkconf
3. Создайте файл <fio>.local.db, содержащий следующие параметры для домена <fio>.local:
    a. Имя основного DNS сервера ns1
    b. E-mail администратора hostmaster@<fio>.local
    c. Серийный номер зоны по шаблону YYYYMMDDhhmm
    d. Время обновления реплики 43200
    e. Время до повторной попытки 3600
    f. Время работы реплики без обновления 3600000
    g. Минимальный TTL 300
    h. Ip адрес ns1 равный внутреннему IP хоста c7-1
    i. Имя gate с IP равным внутреннему IP хоста c7-1
    j. Псевдоним www, направляющий клиента на хост gate.<fio>.local.
4. Для проверки файла зоны используйте утилиту named-checkzone
5. На хосте c7-2 проверьте, что все записи в вашем домене работают

Содержание отчета

Требуется подготовить отчеты в формате DOC\DOCX или PDF. Отчет содержит титульный лист, артефакты выполнения и ответы на вопросы и задания.

Артефакты:

1. Тексты команд и консольные выводы команд Части 2 п.2.
2. Конфигурационный файл /etc/named.conf из Части 3, п.3.
3. Параметры, добавленные в файл /etc/named.conf в Части 4. п. 3.
4. Файл зоны, созданный в Части 4.

Вопросы и задания:

1. Опишите, как в выводе команды dig соотносятся секции HEADER, QUESTION SECTION, ANSWER SECTION, AUTHORITY SECTION, SERVER, WHEN и MSG SIZE с полями секции HEADER. Опишите назначение каждой секции.
2. Как по ответу утилиты dig в Части 3 можно понять, что ответ получен именно от вашего кэширующего DNS сервера?

Отчет выслать в течение 4-х недель на адрес edu-net@yandex.ru.

В теме письма: №группы ФИО (латинскими буквами) №работы (например: 5555 Fedor Sumkin 3)

Поддержка работы

Дополнительные материалы по теме курса публикуются на Telegram-канале ITSMDao (t.me/itsmdao). Обсуждать работу и задавать вопросы можно в чате ITSMDaoChat (t.me/itsmdaochat).