# **Настройка DNS на сервере**

Руководство по настройке DNS сервера предназначена для ОС Ubuntu 22 и новее. Вместо записей DNS\_ИМЯ и IP\_АДРЕС следует подставлять имя вашего домена и ip адрес сервера соответственно.

Вместо записи УЧЕТНАЯ\_ЗАПИСЬ необходимо поставить имя одной из учётных записей на сервере (лучше имя учётной записи администратора, например root или admin). Руководство рассчитано на DNS имена, которые указаны на английском языке (если DNS имя задано на русском, возможно придётся сделать дополнительную настройку сервера).

Вместо записи ТЕКУЩАЯ\_ДАТА необходимо указать текущую дату, например 20240722 (НЕ РЕКОМЕНДУЕТСЯ: если вы меняете конфигурацию впервые и больше не собираетесь менять, можно установить любую цифру, например 2).

Вместо записи ОКТЕТЫ следует подставить первые 3 числа вашего ip адреса, например для адреса 192.168.0.13 следует подставить 192.168.0

Вместо записи ОКТЕТЫ\_НАОБОРОТ следует подставить первые 3 числа вашего ip адреса в обратном порядке, например для адреса 192.168.0.13 следует подставить 0.168.192

Вместо записи ПОСЛЕДНИЙ\_ОКТЕТ нужно подставить последнее число ip адреса. например для адреса 192.168.0.13 следует подставить 13

Обратите внимание, некоторые записи DNS имени в конфигурационных файлах должны заканчиваться точкой.

1) Зайдите в учётную запись администратора (чтобы каждый раз не вводить sudo):

***sudo su (для Ubuntu 24)***

***sudo root (для Ubuntu 22)***

2) Установите DNS-сервер Bind9:

***apt update***

***apt install bind9 -y***

3) Создайте файл зоны для вашего домена.

***mkdir /etc/bind/zones***

***nano /etc/bind/zones/db.DNS\_NAME***

4) Вставьте следующее содержимое в файл зоны:

***$TTL 604800***

***@ IN SOA ns.DNS\_NAME. admin.DNS\_NAME. (***

***ТЕКУЩАЯ\_ДАТА01 ; Serial***

***604800 ; Refresh***

***86400 ; Retry***

***2419200 ; Expire***

***604800 ) ; Negative Cache TTL***

***@ IN NS ns.DNS\_NAME.***

***ns IN A IP\_АДРЕС***

***@ IN A IP\_АДРЕС***

5) Создайте файл зоны обратного просмотра.

***nano /etc/bind/zones/db.ОКТЕТЫ***

6) Вставьте следующее содержимое в файл зоны обратного просмотра

***$TTL 604800***

***@ IN SOA ns.DNS\_NAME. admin.DNS\_NAME. (***

***ТЕКУЩАЯ\_ДАТА01 ; Serial***

***604800 ; Refresh***

***86400 ; Retry***

***2419200 ; Expire***

***604800 ) ; Negative Cache TTL***

***@ IN NS ns.DNS\_ИМЯ.***

***ПОСЛЕДНИЙ\_ОКТЕТ IN PTR DNS\_ИМЯ.***

7) Откройте файл конфигурации Bind для редактирования:

***sudo nano /etc/bind/named.conf.local***

8) Добавьте следующую конфигурацию:

***zone "DNS\_ИМЯ" {***

***type master;***

***file "/etc/bind/zones/db.DNS\_NAME";***

***};***

***zone "ОКТЕТЫ\_НАОБОРОТ.in-addr.arpa" {***

***type master;***

***file "nano /etc/bind/zones/db.ОКТЕТЫ";***

***};***

9) Перезапустите службу Bind9 для применения изменений:

***sudo systemctl restart bind9***

# **Настройка локальной машины Windows для использования вашего DNS-сервера**

1) Запустите текстовый редактор от имени администратора

2) Откройте файл C:\Windows\System32\drivers\etc\hosts

3) Добавьте в конец строку:

***IP\_АДРЕС DNS\_ИМЯ***

# **Настройка локальной машины Ubuntu для использования вашего DNS-сервера**

1) Откройте файл /etc/resolv.conf и добавьте ваш DNS-сервер:

***sudo nano /etc/resolv.conf***

2) Добавьте следующую строку в начало файла:

***nameserver IP\_АДРЕС***

3) Обратите внимание, что изменения в /etc/resolv.conf могут быть временными и сбрасываться после перезагрузки. Чтобы сделать изменения постоянными, настройте файл /etc/systemd/resolved.conf:

***sudo nano /etc/systemd/resolved.conf***

4) Найдите строку DNSStubListener=yes и измените на DNSStubListener=no. Затем найдите строку DNS= и добавьте IP-адрес вашего DNS-сервера:

[Resolve]

***DNS=10.0.2.15***

5) Перезапустите службу systemd-resolved:

***sudo systemctl restart systemd-resolved***

6) Теперь вы можете проверить работу вашего DNS-сервера с помощью команды ping:

***ping DNS\_ИМЯ***

# **Примечания**

Если DNS по-прежнему не работает, значит надо добавить правила в брандмауэр для 53 порта (UDP) и разрешающие правила для ICMP (если ping не идёт даже по ip).

Если на пути к серверу есть сетевое оборудование с листами доступа (ACL), значит туда тоже нужно добавить разрешающие правила.

Также, если в вашей сети развернут VIPnet или подобная технология, то возможно она блокирует DNS трафик.