

# Сервер BIND

BIND (Berkeley Internet Name Domain, до этого: Berkeley Internet Name Daemon) — открытая и наиболее распространённая реализация [DNS](#) сервера.

<https://www.isc.org/downloads/bind/>

⚠ Все примеры для BIND 9

## Установка

```
apt install bind9
```

Создаем файл протокола

```
touch /var/log/named.log; chown bind /var/log/named.log
```

## Настройка

Основная папка	/etc/bind
Папка для размещения slave зон	/var/cache/bind

## Обычный сервер (slave)

### named.conf.local

[named.conf.local](#)

```
include "/etc/bind/zones.rfc1918";
zone "domain.ru" in {
    type slave;
    file "db.domain.ru.slave";
    masters { 192.168.1.1; };
};

zone "1.168.192.in-addr.arpa" in {
    type slave;
    file "db.1.168.192.in-addr.arpa.slave";
    masters { 192.168.1.1; };
};
```

В этом примере описана прямая и обратная зона.

### named.conf.options

[named.conf.options](#)

```
options {
    directory "/var/cache/bind";
    auth-nxdomain no;
    listen-on-v6 { any; };
    listen-on { any; };
};
```

```

        forwarders { 127.0.0.1 port 5353; 8.8.8.8;};
};

logging {
    channel namedlog {
        file "/var/log/named.log";
        severity warning;
        print-time yes;
        print-severity yes;
        print-category yes;
    };
    category default { namedlog; };
    category security { namedlog; };
};

```

Все запросы, которые не смог разрешить это сервер будут опрарлены на 192.168.1.1

Для включения в файл протокола запросов к серверу нужно:

1. Вставить в секцию logging следующую конструкцию:

```

channel "query" {
    file "/var/log/named-query.log" versions 4 size 4m;
    print-time yes;
    print-severity no;
    print-category no;
};
category queries { "query"; };

```

2. Создать файл:

```
touch /var/log/named-query.log; chown bind /var/log/named-query.log
```

3. Перезапустить bind9:

```
service bind9 restart
```

## Главный сервер (master)

### named.conf.local

[named.conf.local](#)

```

include "/etc/bind/zones.rfc1918";

zone "domain.ru" in {
    type master;
    file "/etc/bind/db.domain.ru";
    allow-update { none; };
    allow-transfer { 192.168.1.2; 192.168.1.3;};
};

zone "1.168.192.in-addr.arpa" in {
    type master;
    file "/etc/bind/db.1.168.192";
    allow-update { none; };
    allow-transfer { 192.168.1.2; 192.168.1.3;};
};

```

## named.conf.options

### named.conf.options

```
options {
    directory "/var/cache/bind";
    auth-nxdomain no;
    listen-on-v6 { any; };
    listen-on { any; };
        forwarders { 127.0.0.1 port 5353; 8.8.8.8; };
    allow-recursion { 127.0.0.1; 192.168.1.2; 192.168.1.3; };
};

logging {
    channel namedlog {
        file "/var/log/named.log";
        severity warning;
        print-time yes;
        print-severity yes;
        print-category yes;
    };
    category default { namedlog; };
    category security { namedlog; };
        category update-security { null; };
};
```

Для отключения сообщений определённой категории можно использовать выражение, пример которого приведён ниже:

```
category update-security { null; };
```

[Disable logging for Named/Bind | Linux Support in Adelaide & Melbourne | Redhat Partner](#)

## Прямая зона

### db.domain.ru

```
$ORIGIN .
$TTL 178600      ; 2 days 1 hour 36 minutes 40 seconds
domain.ru IN SOA ns.domain.ru. root.domain.ru. (
    1              ; serial
    28800          ; refresh (8 hours)
    7200           ; retry (2 hours)
    1209600        ; expire (2 weeks)
    7200           ; minimum (2 hours)
)
    NS      ns.domain.ru.
    NS      ns2.domain.ru.
    NS      ns3.domain.ru.
    MX      10 mail.domain.ru.
$ORIGIN domain.ru.
localhost  A      127.0.0.1
ns         A      192.168.1.1
ns2        A      192.168.1.2
ns3        A      192.168.1.3
mail       A      192.168.1.4
ldap       A      192.168.1.2
```

ldap		A	192.168.1.3
webmail	CNAME	mail	
smtp	CNAME	mail	
imap	CNAME	mail	
gate	CNAME	ns	

## Обратная зона

[db.1.168.192](#)

```
$ORIGIN .
$TTL 178600 ; 2 days 1 hour 36 minutes 40 seconds
1.168.192.in-addr.arpa IN SOA ns.domain.ru. root.domain.ru. (
    1 ; serial
    28800 ; refresh (8 hours)
    7200 ; retry (2 hours)
    1209600 ; expire (2 weeks)
    7200 ; minimum (2 hours)
)
NS ns.domain.ru.
$ORIGIN 1.168.192.in-addr.arpa.
1 PTR ns.domain.ru.
2 PTR ns2.domain.ru.
3 PTR ns3.domain.ru.
4 PTR mail.domain.ru.
```

## LDAP



[LDAP](#) back-end plug-in for BIND

```
apt install bind9-dyndb-ldap
```

---

[Migrating zone data to LDAP — bind-dyndb-ldap master documentation](#)

## Ссылки

[Конфигурирование DNS-сервера BIND \(dns bind domain\)](#)

[Bog BOS: DNS сервер BIND](#)

[Split DNS: заставим BIND работать на два фронта!](#)

[Настройка логов Bind9 — IT Blog](#)

<http://sysadminmosaic.ru/bind/bind>

2020-08-13 09:11

