

Лабораторная работа №3

Настройка DHCP-сервера KEA и интеграция с DNS

Владимир Базлов

14 ноября 2025

Российский университет дружбы народов, Москва, Россия

Цель работы

Основная цель

Получить практические навыки настройки DHCP-сервера Kea,
а также реализовать динамическое обновление DNS-зон (**DDNS**)
с использованием Bind9 и TSIG-ключей.

Конфигурирование DHCP-сервера

Изменение доменных параметров

```
kea-dhcp4.conf      [-M--]  0 L:[145+ 9 154/460] *(7500/21790b) 0010 0x00A
    //      "csv-format": "true",
    //      "space": "dhcp4",
    //      "data": "192.0.2.1, 192.0.2.2"
    // }
    // but it's a lot of writing, so it's easier to do this instead:
    {
        "name": "domain-name-servers",
        "data": "192.168.1.1"
    },
    {
        "code": 15,
        "data": "vabazlov.net"
    },
    {
        "name": "domain-search",
        "data": "vabazlov.net"
    },
```

Рис. 1: Редактирование kea-dhcp4.conf

Настройка подсети

```
// structures.
"subnet4": [
{
    "id": 1,
    "subnet": "192.168.1.0/24",
    "pools": [ { "pool": "192.168.1.30 - 192.168.1.199" } ],
    "option-data": [
        {
            "name": "routers",
            "data": "192.168.1.1"
        }
    ]
},
],
// There are many, many more parameters that DHCPv4 server is able to use.
// They were not added here to not overwhelm people with too much
// information at once.
```

Рис. 2: Конфигурирование подсети

Проверка и включение службы

```
[root@server.vabazlov.net ~]# kea-dhcp4 -t /etc/kea/kea-dhcp4.conf
2025-11-14 08:59:25.598 INFO [kea-dhcp4.hosts/14507.140125840922816] HOSTS_BACKENDS_REGISTERED the following host backend types are available: mysql postgresql
2025-11-14 08:59:25.599 WARN [kea-dhcp4.dhcpsrv/14507.140125840922816] DHCPSRV_MT_DISABLED_QUEUE_CONTROL disabling dhcp queue control when multi-threading is enabled.
2025-11-14 08:59:25.599 WARN [kea-dhcp4.dhcp4/14507.140125840922816] DHCP4_RESERVATIONS_LOOKUP_FIRST_ENABLED Multi-threading is enabled and host reservations lookup is always performed first.
2025-11-14 08:59:25.599 INFO [kea-dhcp4.dhcpsrv/14507.140125840922816] DHCPSRV_CFGMGR_NEW_SUBNET4 a new subnet has been added to configuration: 192.168.1.0/24 with params: t1=900, t2=1800, valid-lifetime=3600
2025-11-14 08:59:25.599 INFO [kea-dhcp4.dhcpsrv/14507.140125840922816] DHCPSRV_CFGMGR_SOCKET_TYPE_SELECT using socket type raw
2025-11-14 08:59:25.599 INFO [kea-dhcp4.dhcpsrv/14507.140125840922816] DHCPSRV_CFMGR_ADD_IFACE listening on interface eth1
2025-11-14 08:59:25.599 INFO [kea-dhcp4.dhcpsrv/14507.140125840922816] DHCPSRV_CFGMGR_SOCKET_TYPE_DEFAULT "dhcp-socket-type" not specified , using default socket type raw
[root@server.vabazlov.net ~]#
[root@server.vabazlov.net ~]# systemctl --system daemon-reload
Unknown command verb 'daemon-re', did you mean 'daemon-reload'?
[root@server.vabazlov.net ~]# systemctl --system daemon-reload
[root@server.vabazlov.net ~]# systemctl enable kea-dhcp4.service
Created symlink '/etc/systemd/system/multi-user.target.wants/kea-dhcp4.service' → '/usr/lib/systemd/system/kea-dhcp4.service'.
[root@server.vabazlov.net ~]#
```

Рис. 3: systemctl действия

Добавление записей в зоны

```
vabazlov.net      [----] 42 L:[ 1+ 5   6/ 14] *(108 / 238b) 0009 0x009
$TTL 1D
@<---->IN SOA<>@ server.vabazlov.net. (
<----><----><----><----><---->2025111400<---->; serial
<----><----><----><----><---->1D<---->; refresh
<----><----><----><----><---->1H<---->; retry
<----><----><----><----><---->1W<---->; expire
<----><----><----><----><---->3H )<--->; minimum
<---->NS<---->@
<---->A<---->192.168.1.1
$ORIGIN vabazlov.net.
server<>A<---->192.168.1.1
ns<---->A<---->192.168.1.1
dhcp<-->A<---->192.168.1.1
```

Рис. 4: Прямая зона

Добавление записей в зоны

```
192.168.1      [----] 48 L:[ 1+ 2   3/ 15] *(55 / 293b) 0048 0x030
$TTL 1D
@<---->IN SOA<>@ server.vabazlov.net. (
<----><----><----><----><---->20251114000<---->; serial
<----><----><----><----><---->1D<---->; refresh
<----><----><----><----><---->1H<---->; retry
<----><----><----><----><---->1W<---->; expire
<----><----><----><----><---->3H )<---->; minimum
<---->NS<---->@
<---->A<---->192.168.1.1
<---->PTR<---->server.vabazlov.net.
$ORIGIN 1.168.192.in-addr.arpa.
1<---->PTR<---->server.vabazlov.net.
1<---->PTR<---->ns.vabazlov.net.
1<---->PTR<---->dhcp.vabazlov.net.
```

Рис. 5: Обратная зона

Проверка работы DNS

```
[root@server.vabazlov.net ~]#  
[root@server.vabazlov.net ~]# systemctl restart named  
[root@server.vabazlov.net ~]#  
[root@server.vabazlov.net ~]# ping dhcp.vabazlov.net  
PING dhcp.vabazlov.net (192.168.1.1) 56(84) bytes of data.  
64 bytes from dhcp.vabazlov.net (192.168.1.1): icmp_seq=1 ttl=64 time=0.015 ms  
64 bytes from dhcp.vabazlov.net (192.168.1.1): icmp_seq=2 ttl=64 time=0.097 ms  
64 bytes from dhcp.vabazlov.net (192.168.1.1): icmp_seq=3 ttl=64 time=0.090 ms  
64 bytes from dhcp.vabazlov.net (192.168.1.1): icmp_seq=4 ttl=64 time=0.073 ms  
64 bytes from dhcp.vabazlov.net (192.168.1.1): icmp_seq=5 ttl=64 time=0.091 ms  
64 bytes from dhcp.vabazlov.net (192.168.1.1): icmp_seq=6 ttl=64 time=0.087 ms  
64 bytes from dhcp.vabazlov.net (192.168.1.1): icmp_seq=7 ttl=64 time=0.043 ms  
64 bytes from dhcp.vabazlov.net (192.168.1.1): icmp_seq=8 ttl=64 time=0.064 ms  
64 bytes from dhcp.vabazlov.net (192.168.1.1): icmp_seq=9 ttl=64 time=0.072 ms  
64 bytes from dhcp.vabazlov.net (192.168.1.1): icmp_seq=10 ttl=64 time=0.054 ms  
^C  
--- dhcp.vabazlov.net ping statistics ---  
10 packets transmitted, 10 received, 0% packet loss, time 9234ms  
rtt min/avg/max/mdev = 0.015/0.068/0.097/0.024 ms  
[root@server.vabazlov.net ~]#
```

Рис. 6: Проверка

Выдача адреса

```
vabazlov@client:~  
RX packets 1968 bytes 237058 (231.5 KiB)  
RX errors 0 dropped 0 overruns 0 frame 0  
TX packets 1696 bytes 271332 (264.9 KiB)  
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0  
  
eth1: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500  
    inet 192.168.1.30 netmask 255.255.255.0 broadcast 192.168.1.255  
    inet6 fe80::8f0:fda6:1c54:1604 prefixlen 64 scopeid 0x20<link>  
        ether 08:00:27:17:33:c0 txqueuelen 1000 (Ethernet)  
        RX packets 74 bytes 7681 (7.5 KiB)  
        RX errors 0 dropped 0 overruns 0 frame 0  
        TX packets 251 bytes 23698 (23.1 KiB)  
        TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0  
  
lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536  
    inet 127.0.0.1 netmask 255.0.0.0  
    inet6 ::1 prefixlen 128 scopeid 0x10<host>  
        loop txqueuelen 1000 (Local Loopback)  
        RX packets 18 bytes 2112 (2.0 KiB)  
        RX errors 0 dropped 0 overruns 0 frame 0  
        TX packets 18 bytes 2112 (2.0 KiB)  
        TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0  
  
[vabazlov@client.vabazlov.net ~]$
```

Запись аренды

```
[root@server.vabazlov.net ~]#  
[root@server.vabazlov.net ~]# cat /var/lib/kea/kea-leases4.csv  
address,hwaddr,client_id,valid_lifetime,expire,subnet_id,fqdn_fwd,fqdn_rev,hostname,state,user_context,pool_id  
192.168.1.30,08:00:27:17:33:c0,01:08:00:27:17:33:c0,3600,1763114833,1,0,0,client,,0  
192.168.1.30,08:00:27:17:33:c0,01:08:00:27:17:33:c0,3600,1763114833,1,0,0,client,,0  
192.168.1.30,08:00:27:17:33:c0,01:08:00:27:17:33:c0,3600,1763114838,1,0,0,client,,0  
[root@server.vabazlov.net ~]#
```

Рис. 8: lease файл

Генерация TSIG-ключа

```
[root@server.vabazlov.net ~]#  
[root@server.vabazlov.net ~]# mkdir -p /etc/named/keys  
[root@server.vabazlov.net ~]# tsig-keygen -a HMAC-SHA512 DHCP_UPDATER > /etc/named/keys/dhcp_updater.key  
[root@server.vabazlov.net ~]# cat /etc/named/keys/dhcp_updater.key  
key "DHCP_UPDATER" {  
    algorithm hmac-sha512;  
    secret "bwrQJSj0VLdspEgjSzQHndxJK/SFvGfEktNBEenqz8mqBvH7ukjCI1WGcdSvgl5vvVyzWq9oGjg3A+PjJSOCvg=";  
};  
[root@server.vabazlov.net ~]# chown -R named:named /etc/named/keys  
[root@server.vabazlov.net ~]# █
```

Рис. 9: Создание ключа

Разрешение обновлений зон

```
vabazlov.net      [-M--] 10 L:[ 1+29 30/ 33] *(813 / 818b) 0010 0x00A
// named.rfc1912.zones:
//
// Provided by Red Hat caching-nameserver package.
//
// ISC BIND named zone configuration for zones recommended by
// RFC 1912 section 4.1 : localhost TLDs and address zones
// and https://tools.ietf.org/html/rfc6303
// (c)2007 R W Franks
//.
// See /usr/share/doc/bind*/sample/ for example named configuration files.
//
// Note: empty-zones-enable yes; option is default.
// If private ranges should be forwarded, add.
// disable-empty-zone "."; into options
//.

zone "vabazlov.net" IN {
    type master;
    file "master/fz/vabazlov.net";
    update-policy {
        grant DHCP_UPDATER wildcard *.vabazlov.net A DHCID;
    };
};

zone "1.168.192.in-addr.arpa" IN {
    type master;
    file "master/rz/192.168.1";
    update-policy {
        grant DHCP_UPDATER wildcard *.1.168.192.in-addr.arpa PTR DHCID;
    };
};
```

Подготовка ключа для Kea

```
tsig-keys.json      [---] 2 L:[ 1+ 6 7/ 8] *(185 / 186b) 0010 0x00A
[{"name": "DHCP_UPDATER", "algorithm": "hmac-sha512", "secret": "bwriQJ5jJ0VLdspLtgSzQHndxJK/SFvGFEktNBEnqz8mqBvH7ukjCIIWGCdSvgl5vvVyzWq9o0jg3A+PjJSOCvg**"}]
```

Рис. 11: tsig-keys.json

Настройка Kea DHCP-DDNS

```
kea-dhcp-ddns.conf [BM--] 32 L:[ 20+27 47/100] *(1605/3398b) 0010 0x0A
"DhcpDdns":
{
    "ip-address": "127.0.0.1",
    "port": 53001,
    "control-socket": {
        "socket-type": "unix",
        "socket-name": "/run/kea/kea-ddns-ctrl-socket"
    },
    <?include "/etc/kea/tsig-keys.json"?>

    "forward-ddns" : {
        "ddns-domains" : [
            {
                "name": "vabazlov.net.",
                "key-name": "DHCP_UPDATER",
                "dns-servers": [
                    { "ip-address": "192.168.1.1" }
                ]
            }
        ],
    },
    "reverse-ddns" : {
        "ddns-domains" : [
            {
                "name": "1.168.192.in-addr.arpa.",
                "key-name": "DHCP_UPDATER",
                "dns-servers": [
                    { "ip-address": "192.168.1.1" }
                ]
            }
        ],
    },
}
```

Запуск службы DDNS

```
[root@server.vabazlov.net ~]#  
[root@server.vabazlov.net ~]# kea-dhcp-ddns -t /etc/kea/kea-dhcp-ddns.conf  
2025-11-14 09:43:00.985 INFO  [kea-dhcp-ddns.dctl/22417.140373503476032] DCTL_CONFIG_CHECK_COMPL  
ETE server has completed configuration check: listening on 127.0.0.1, port 53001, using UDP, res  
ult: success(0), text=Configuration check successful  
[root@server.vabazlov.net ~]# systemctl enable --now kea-dhcp-ddns.service  
Created symlink '/etc/systemd/system/multi-user.target.wants/kea-dhcp-ddns.service' → '/usr/lib/  
systemd/system/kea-dhcp-ddns.service'.  
[root@server.vabazlov.net ~]# systemctl status --now kea-dhcp-ddns.service  
● kea-dhcp-ddns.service - Kea DHCP-DDNS Server  
   Loaded: loaded (/usr/lib/systemd/system/kea-dhcp-ddns.service; enabled; preset: disabled)  
   Active: active (running) since Fri 2025-11-14 09:43:32 UTC; 7s ago  
     Invocation: a257e333d64e4c7da831d035693f555b  
       Docs: man:kea-dhcp-ddns(8)  
     Main PID: 22676 (kea-dhcp-ddns)  
        Tasks: 5 (limit: 10381)  
      Memory: 1.8M (peak: 6.1M)  
        CPU: 10ms  
      CGroup: /system.slice/kea-dhcp-ddns.service  
              └─22676 /usr/sbin/kea-dhcp-ddns -c /etc/kea/kea-dhcp-ddns.conf  
  
Nov 14 09:43:32 server.vabazlov.net systemd[1]: Started kea-dhcp-ddns.service - Kea DHCP-DDNS S>  
Nov 14 09:43:32 server.vabazlov.net kea-dhcp-ddns[22676]: 2025-11-14 09:43:32.588 INFO  [kea-dh>  
Nov 14 09:43:32 server.vabazlov.net kea-dhcp-ddns[22676]: INFO  COMMAND_ACCEPTOR_START Starting>  
Nov 14 09:43:32 server.vabazlov.net kea-dhcp-ddns[22676]: INFO  DCTL_CONFIG_COMPLETE server has>
```

Рис. 13: Статус ddns

Включение DDNS в Kea DHCP

```
kea-dhcp4.conf      [---] 30 L:[ 36+20  56/351] *(2966/16048b) 0010 0x00A
    // Kea DHCPv4 server by default listens using raw sockets. This ensures
    // all packets, including those sent by directly connected clients
    // that don't have IPv4 address yet, are received. However, if your
    // traffic is always relayed, it is often better to use regular
    // UDP sockets. If you want to do that, uncomment this line:
    // "dhcp-socket-type": "udp"
    },

    "dhcp-ddns" : {
<----->"enable-updates": true
    },
    "ddns-qualifying-suffix": "vabazlov.net",
    "ddns-override-client-update": true,
    // Kea supports control channel, which is a way to receive management
    // commands while the server is running. This is a Unix domain socket that
    // receives commands formatted in JSON, e.g. config-set (which sets new
    // configuration), config-reload (which tells Kea to reload its
    // configuration from file), statistic-get (to retrieve statistics) and many
    // more. For detailed description, see Sections 8.8, 16 and 15.
    "control-socket": {
        "socket-type": "unix",
        "socket-name": "kea4-ctrl-socket"
    },
}
```

Рис. 14: kea-dhcp4 изменения

Проверка результата

```
[vabazlov@client.vabazlov.net ~]$ dig @192.168.1.1 client.vabazlov.net

; <>> DiG 9.18.33 <>> @192.168.1.1 client.vabazlov.net
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 14313
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: 70c7f539d10080f3010000006916fac18f5ce3e4a6901544 (good)
;; QUESTION SECTION:
;client.vabazlov.net.      IN      A

;; ANSWER SECTION:
client.vabazlov.net.    1200    IN      A      192.168.1.30

;; Query time: 1 msec
;; SERVER: 192.168.1.1#53(192.168.1.1) (UDP)
;; WHEN: Fri Nov 14 09:47:46 UTC 2025
;; MSG SIZE  rcvd: 92

[vabazlov@client.vabazlov.net ~]$ █
```

Рис. 15: dig client.vabazlov.net

Итоги работы

В результате выполнения лабораторной работы:

- Настроен DHCP-сервер Kea на выдачу сетевых параметров.
- Реализована интеграция DHCP с Bind9 через DDNS.
- Настроены TSIG-ключи и безопасность взаимодействия.
- Подтверждена работа автоматического создания A- и PTR-записей.
- Подготовлены provisioning-скрипты для автоматизации настройки.
- Клиентские машины корректно получают настройки и DNS-записи.

Настройка завершена успешно, инфраструктура функционирует стablyно.