Администрирование системных подсистем

Настройка DHCP-сервера Kea и интеграция с DNS (Bind9 + DDNS)

Сейдалиев Тагиетдин Ровшенович

19 ноября 2025

Российский университет дружбы народов, Москва, Россия

Цель работы

Основная цель

Приобретение практических навыков настройки DHCP-сервера Kea
и интеграции его с DNS Bind9, включая механизм динамических обновлений DDNS.

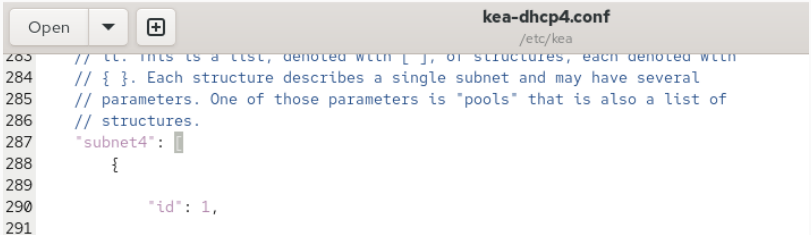
Конфигурирование DHCP-сервера

Настройка параметров домена

- Обновлены `domain-name`, `domain-search`
- DNS-сервер: `192.168.1.1`
- Внесены изменения в файл `/etc/kea/kea-dhcp4.conf`

Настройка подсети DHCP

- Сеть: `192.168.1.0/24`
- Диапазон: `192.168.1.30–192.168.1.199`
- Шлюз: `192.168.1.1`



Проверка работы службы DHCP

- Проверка корректности конфигурации
- Перезапуск сервиса
- Включение автозагрузки

```
[root@server.trseidaliev.net server]#
[root@server.trseidaliev.net server]# kea-dhcp4 -t /etc/kea/kea-dhcp4.conf
2025-11-19 19:00:06.379 INFO  [kea-dhcp4.hosts/21246.139875138164928] HOSTS_BACKENDS_REGISTERED the following host bac
kend types are available: mysql postgresql
2025-11-19 19:00:06.380 WARN  [kea-dhcp4.dhcpsrv/21246.139875138164928] DHCPSRV_MT_DISABLED_QUEUE_CONTROL disabling dh
cp queue control when multi-threading is enabled.
2025-11-19 19:00:06.380 WARN  [kea-dhcp4.dhcp4/21246.139875138164928] DHCP4_RESERVATIONS_LOOKUP_FIRST_ENABLED Multi-th
reading is enabled and host reservations lookup is always performed first.
2025-11-19 19:00:06.381 INFO  [kea-dhcp4.dhcpsrv/21246.139875138164928] DHCPSRV_CFGMGR_NEW_SUBNET4 a new subnet has be
en added to configuration: 192.168.1.0/24 with params: t1=900, t2=1800, valid-lifetime=3600
2025-11-19 19:00:06.381 INFO  [kea-dhcp4.dhcpsrv/21246.139875138164928] DHCPSRV_CFGMGR_SOCKET_TYPE_SELECT using socket
 type raw
2025-11-19 19:00:06.381 INFO  [kea-dhcp4.dhcpsrv/21246.139875138164928] DHCPSRV_CFGMGR_ADD_IFACE listening on interfac
e eth1
2025-11-19 19:00:06.381 INFO  [kea-dhcp4.dhcpsrv/21246.139875138164928] DHCPSRV_CFGMGR_SOCKET_TYPE_DEFAULT "dhcp-socke
t-type" not specified , using default socket type raw
[root@server.trseidaliev.net server]# systemctl --system daemon-reload
[root@server.trseidaliev.net server]# systemctl enable kea-dhcp4.service
Created symlink '/etc/systemd/system/multi-user.target.wants/kea-dhcp4.service' → '/usr/lib/systemd/system/kea-dhcp4.s
ervice'.
[root@server.trseidaliev.net server]#
```

Настройка DNS-зон

Прямая зона

Добавлена A-запись для DHCP-сервера и обновлён серийный номер зоны.

Open

trseidaliev.net
/var/named/master/fz

```
1  $TTL 1D
2  @       IN SOA  @ server.trseidaliev.net. (
3                                           2025111900      ; serial
4                                           1D      ; refresh
5                                           1H      ; retry
6                                           1W      ; expire
7                                           3H )    ; minimum
8          NS      @
9          A       192.168.1.1
10 $ORIGIN trseidaliev.net.
11 server  A       192.168.1.1
12 ns      A       192.168.1.1
13 dhcp    A       192.168.1.1
14
```

Рис. 4: Файл прямой зоны после изменения

Обратная зона

Добавлена PTR-запись и обновлён SOA serial.

Open

192.168.1
/var/named/master/rz

```
$TTL 1D
@       IN SOA  @ server.trseidaliev.net. (
                                        2025111900      ; serial
                                        1D      ; refresh
                                        1H      ; retry
                                        1W      ; expire
                                        3H )    ; minimum
        NS      @
        A       192.168.1.1
        AAAA    ::1
        PTR     server.trseidaliev.net.
$ORIGIN 1.168.192.in-addr.arpa.
1       PTR     server.trseidaliev.net.
1       PTR     ns.trseidaliev.net.
1       PTR     dhcp.trseidaliev.net.

```

Рис. 5: Файл обратной зоны

Проверка сетевого взаимодействия

Проверка имени DHCP-узла

```
[root@server.trseidaliev.net server]#
[root@server.trseidaliev.net server]# systemctl restart named
[root@server.trseidaliev.net server]#
[root@server.trseidaliev.net server]# ping dhcp.trseidaliev.net
PING dhcp.trseidaliev.net (192.168.1.1) 56(84) bytes of data.
64 bytes from server.trseidaliev.net (192.168.1.1): icmp_seq=1 ttl=64 time=0.012 ms
64 bytes from server.trseidaliev.net (192.168.1.1): icmp_seq=2 ttl=64 time=0.084 ms
64 bytes from server.trseidaliev.net (192.168.1.1): icmp_seq=3 ttl=64 time=0.037 ms
64 bytes from server.trseidaliev.net (192.168.1.1): icmp_seq=4 ttl=64 time=0.064 ms
64 bytes from server.trseidaliev.net (192.168.1.1): icmp_seq=5 ttl=64 time=0.061 ms
64 bytes from server.trseidaliev.net (192.168.1.1): icmp_seq=6 ttl=64 time=0.077 ms
^C
--- dhcp.trseidaliev.net ping statistics ---
6 packets transmitted, 6 received, 0% packet loss, time 5577ms
rtt min/avg/max/mdev = 0.012/0.055/0.084/0.024 ms
[root@server.trseidaliev.net server]#
```

Рис. 6: Проверка ping по имени dhcp..net

- Разрешена служба DHCP
- Восстановлены контексты SELinux `/etc`, `/var/named`, `/var/lib/kea`

```
[root@server.trseidaliev.net server]#
[root@server.trseidaliev.net server]# firewall-cmd --add-service=dhcp
success
[root@server.trseidaliev.net server]# firewall-cmd --add-service=dhcp --permanent
success
[root@server.trseidaliev.net server]# restorecon -vR /etc
[root@server.trseidaliev.net server]# restorecon -vR /var/named/
[root@server.trseidaliev.net server]# restorecon -vR /var/lib/kea/
[root@server.trseidaliev.net server]# systemctl start kea-dhcp4.service
[root@server.trseidaliev.net server]#
```

Рис. 7: Изменения в firewall и SELinux

Анализ работы DHCP-сервера

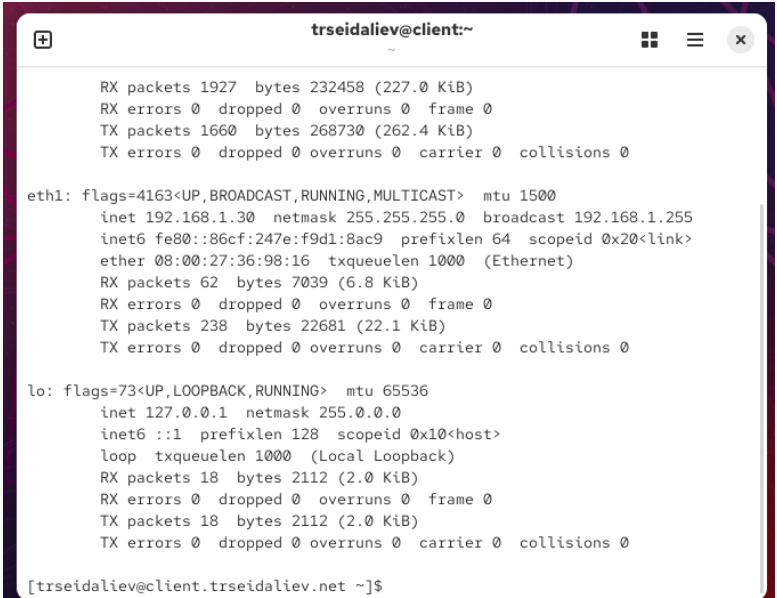
Скрипт маршрутизации клиента

Vagrantfile | dns.sh | 01-routing.sh

```
#!/bin/bash

echo "Provisioning script $0"

nmcli connection modify "eth1" ipv4.gateway "192.168.1.1"
nmcli connection up "eth1"

nmcli connection modify eth0 ipv4.never-default true
nmcli connection modify eth0 ipv6.never-default true

nmcli connection down eth0
nmcli connection up eth0

# systemctl restart NetworkManager
```

Рис. 8: Скрипт настройки маршрутизации клиента

Получение IP-адреса клиентом



Журнал аренд Kea

```
[root@server.trseidaliev.net server]#
[root@server.trseidaliev.net server]# 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
192.168.1.30,08:00:27:36:98:16,01:08:00:27:36:98:16,3600,1763571977,1,0,0,client,0,,0
192.168.1.30,08:00:27:36:98:16,01:08:00:27:36:98:16,3600,1763571977,1,0,0,client,0,,0
192.168.1.30,08:00:27:36:98:16,01:08:00:27:36:98:16,3600,1763571982,1,0,0,client,0,,0
[root@server.trseidaliev.net server]#
```

Рис. 10: Содержимое файла kea-leases4.csv

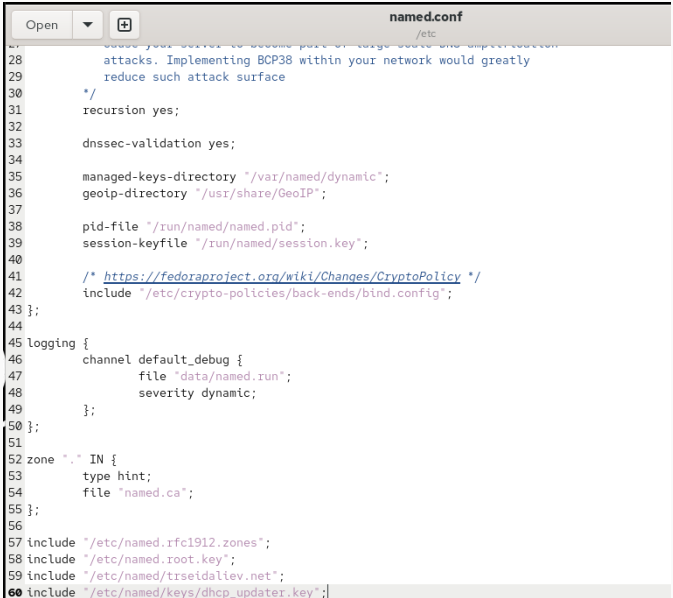
Настройка DDNS

Генерация TSIG-ключа

```
[root@server.trseidaliev.net server]#
[root@server.trseidaliev.net server]# mkdir -p /etc/named/keys
[root@server.trseidaliev.net server]# tsig-keygen -a HMAC-SHA512 DHCP_UPDATER > /etc/named/keys/dhcp_updater.key
[root@server.trseidaliev.net server]# cat /etc/named/keys/dhcp_updater.key
key "DHCP_UPDATER" {
        algorithm hmac-sha512;
        secret "vn63cmyZgm5UQRNJsOfeoxh5aWl//QexHcWouly6Kn6IuLJBvEvQO/RIWTad/lkdBShKiVa+OmwAa3AGyoSrlA==";
};
[root@server.trseidaliev.net server]# chown -R named:named /etc/named/keys/
[root@server.trseidaliev.net server]#
```

Рис. 11: Создание ключа DHCP_UPDATER

Включение ключа в named.conf



Разрешения на обновления зоны

Open

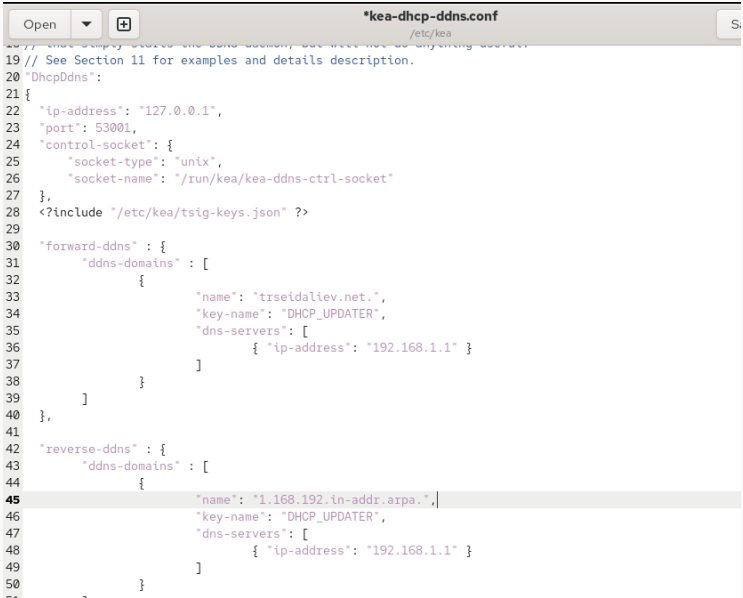
trseidaliev.net
/etc/named

```
// 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 "trseidaliev.net" IN {
        type master;
        file "master/fz/trseidaliev.net";
        update-policy {
                grant DHCP_UPDATER wildcard *.trseidaliev.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;
        };
};
```

Разрешения на обновления зоны

Рис. 14: Разрешение обновлений в обратной зоне

Настройка tsig-keys.json



Настройка kea-dhcp-ddns.conf

```
[root@server.trseidaliev.net server]#
[root@server.trseidaliev.net server]# kea-dhcp-ddns -t /etc/kea/kea-dhcp-ddns.conf
2025-11-19 19:21:41.818 INFO  [kea-dhcp-ddns.dctl/24626.140596514251072] DCTL_CONFIG_CHECK_COMPLETE server has complet
ed configuration check: listening on 127.0.0.1, port 53001, using UDP, result: success(0), text=Configuration check su
ccessful
[root@server.trseidaliev.net server]# 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-dhc
p-ddns.service'.
[root@server.trseidaliev.net server]# systemctl status 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 Wed 2025-11-19 19:22:08 MSK; 13s ago
 Invocation: 0fe992799394887969997b06645d8ef
       Docs: man:kea-dhcp-ddns(8)
   Main PID: 24872 (kea-dhcp-ddns)
      Tasks: 5 (limit: 10381)
     Memory: 1.7M (peak: 6.1M)
        CPU: 10ms
     CGroup: /system.slice/kea-dhcp-ddns.service
             └─24872 /usr/sbin/kea-dhcp-ddns -c /etc/kea/kea-dhcp-ddns.conf

Nov 19 19:22:08 server.trseidaliev.net systemd[1]: Started kea-dhcp-ddns.service - Kea DHCP-DDNS Server.
Nov 19 19:22:08 server.trseidaliev.net kea-dhcp-ddns[24872]: 2025-11-19 19:22:08.247 INFO  [kea-dhcp-ddns.dctl/24872.>
Nov 19 19:22:08 server.trseidaliev.net kea-dhcp-ddns[24872]: INFO  COMMAND_ACCEPTOR_START Starting to accept connecti>
Nov 19 19:22:08 server.trseidaliev.net kea-dhcp-ddns[24872]: INFO  DCTL_CONFIG_COMPLETE server has completed configur>
Nov 19 19:22:08 server.trseidaliev.net kea-dhcp-ddns[24872]: INFO  DHCP_DDNS_STARTED Kea DHCP-DDNS server version 2.6>
lines 1-17/17 (END)
```

Рис. 16: Фрагмент kea-dhcp-ddns.conf

Запуск службы DDNS

Open

kea-dhcp4.conf

/etc/kea

```
// and will be ignored by other components.
"Dhcp4": {
    // Add names of your network interfaces to listen on.
    "interfaces-config": {
        // See section 8.2.4 for more details. You probably want to add just
        // interface name (e.g. "eth0" or specific IPv4 address on that
        // interface name (e.g. "eth0/192.0.2.1").
        "interfaces": [ "eth1" ]

        // 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": "trseidaliev.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
```

Включение DDNS в DHCP4

```
[root@server.trseidaliev.net server]# kea-dhcp4 -t  /etc/kea/kea-dhcp4.conf
2025-11-19 19:24:27.584 INFO  [kea-dhcp4.hosts/25203.139864501876928] HOSTS_BACKENDS_REGISTERED the following host bac
kend types are available: mysql postgresql
2025-11-19 19:24:27.585 WARN  [kea-dhcp4.dhcpsrv/25203.139864501876928] DHCPSRV_MT_DISABLED_QUEUE_CONTROL disabling dh
cp queue control when multi-threading is enabled.
2025-11-19 19:24:27.585 WARN  [kea-dhcp4.dhcp4/25203.139864501876928] DHCP4_RESERVATIONS_LOOKUP_FIRST_ENABLED Multi-th
reading is enabled and host reservations lookup is always performed first.
2025-11-19 19:24:27.585 INFO  [kea-dhcp4.dhcpsrv/25203.139864501876928] DHCPSRV_CFGMGR_NEW_SUBNET4 a new subnet has be
en added to configuration: 192.168.1.0/24 with params: t1=900, t2=1800, valid-lifetime=3600
2025-11-19 19:24:27.585 INFO  [kea-dhcp4.dhcpsrv/25203.139864501876928] DHCPSRV_CFGMGR_SOCKET_TYPE_SELECT using socket
 type raw
2025-11-19 19:24:27.585 INFO  [kea-dhcp4.dhcpsrv/25203.139864501876928] DHCPSRV_CFGMGR_ADD_IFACE listening on interfac
e eth1
2025-11-19 19:24:27.585 INFO  [kea-dhcp4.dhcpsrv/25203.139864501876928] DHCPSRV_CFGMGR_SOCKET_TYPE_DEFAULT "dhcp-socke
t-type" not specified , using default socket type raw
[root@server.trseidaliev.net server]#
[root@server.trseidaliev.net server]# systemctl restart kea-dhcp4.service
[root@server.trseidaliev.net server]# systemctl status kea-dhcp4.service
● kea-dhcp4.service - Kea DHCPv4 Server
     Loaded: loaded (/usr/lib/systemd/system/kea-dhcp4.service; enabled; preset: disabled)
     Active: active (running) since Wed 2025-11-19 19:24:41 MSK; 5s ago
 Invocation: cb7e5da1c0e840fb954f99de7c5ce3c3
       Docs: man:kea-dhcp4(8)
   Main PID: 25273 (kea-dhcp4)
      Tasks: 7 (limit: 10381)
     Memory: 2.5M (peak: 6M)
        CPU: 13ms
     CGroup: /system.slice/kea-dhcp4.service
             └─25273 /usr/sbin/kea-dhcp4 -c /etc/kea/kea-dhcp4.conf

Nov 19 19:24:41 server.trseidaliev.net systemd[1]: Started kea-dhcp4.service - Kea DHCPv4 Server.
Nov 19 19:24:41 server.trseidaliev.net kea-dhcp4[25273]: 2025-11-19 19:24:41.161 INFO  [kea-dhcp4.dhcp4/25273.1399095>
Nov 19 19:24:41 server.trseidaliev.net kea-dhcp4[25273]: 2025-11-19 19:24:41.161 INFO  [kea-dhcp4.commands/25273.1399>
lines 1-15/15 (END)
```

Проверка DDNS

Проверка A-записи, созданной автоматически

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

; <<>> DiG 9.18.33 <<>> @192.168.1.1 client.trseidaliev.net
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 58475
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: 129fa27f46fdda9e01000000691def862038615073907298 (good)
;; QUESTION SECTION:
;client.trseidaliev.net.                IN      A

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

;; Query time: 1 msec
;; SERVER: 192.168.1.1#53(192.168.1.1) (UDP)
;; WHEN: Wed Nov 19 16:30:50 UTC 2025
;; MSG SIZE  rcvd: 95

[trseidaliev@client.trseidaliev.net ~]$
```

Итоги работы

Основные результаты

- Настроен DHCP-сервер Kea с автоматической выдачей IP
- Настроены прямые и обратные зоны Bind9
- Реализован механизм DDNS с TSIG
- Проверены A- и PTR-записи, создаваемые автоматически
- Перенесены конфигурации в структуру Vagrant
- Создан сценарий `dhcp.sh` для автоматического развёртывания