Администрирование сетевых подсистем

Лабораторная работа №3

Чилеше Лупупа

2025

Российский университет дружбы народов, Москва, Россия

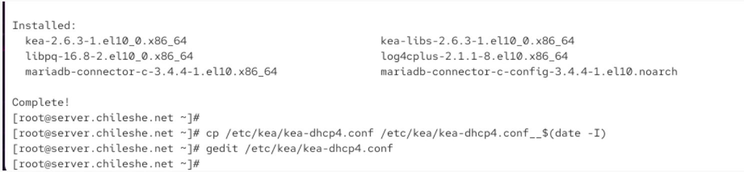
Цель работы

Основная цель

Приобретение навыков по установке и конфигурированию DHCP-сервера Kea, а также интеграции его с DNS-сервером Bind9 с поддержкой динамических обновлений (DDNS).

Выполнение работы

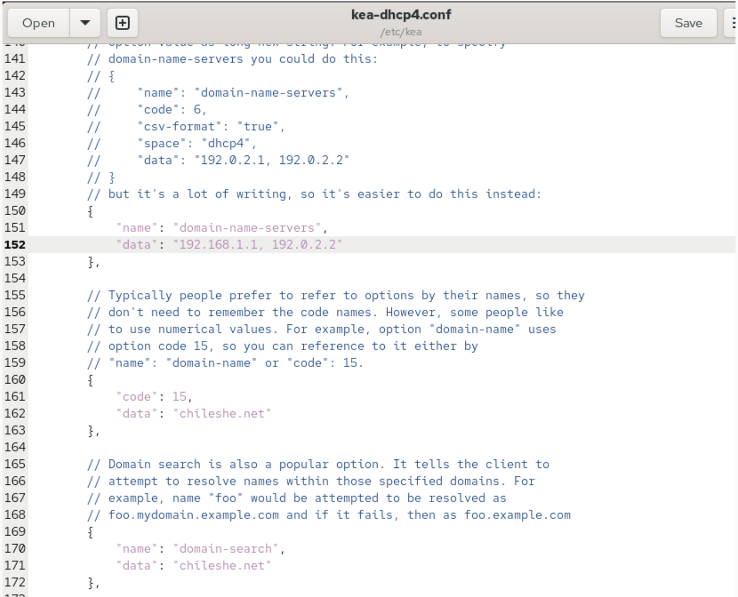
Резервное копирование конфигурации



```
Installed:
  kea-2.6.3-1.el10_0.x86_64                             kea-libs-2.6.3-1.el10_0.x86_64
  libpq-16.8-2.el10_0.x86_64                            log4cplus-2.1.1-8.el10.x86_64
  mariadb-connector-c-3.4.4-1.el10.x86_64               mariadb-connector-c-config-3.4.4-1.el10.noarch

Complete!
[root@server.chileshe.net ~]#
[root@server.chileshe.net ~]# cp /etc/kea/kea-dhcp4.conf /etc/kea/kea-dhcp4.conf__$(date -I)
[root@server.chileshe.net ~]# gedit /etc/kea/kea-dhcp4.conf
[root@server.chileshe.net ~]#
```

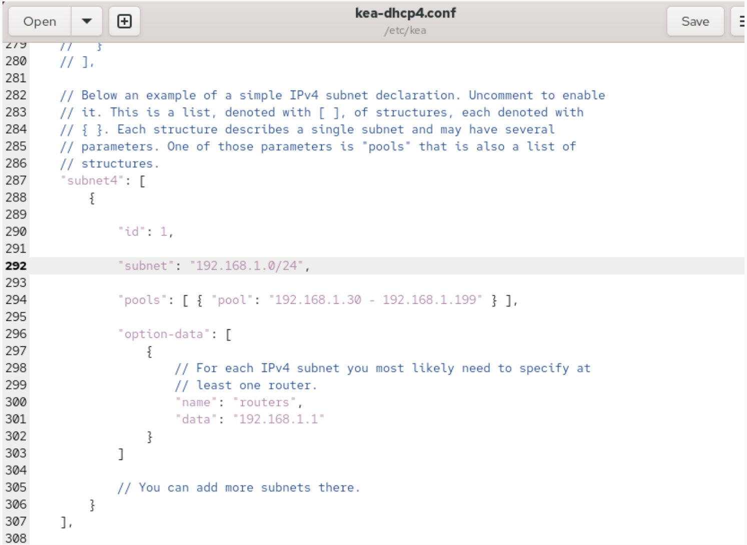
Рис. 1: Резервное копирование конфигурации

Изменение конфигурации DHCP



```
        // option value as long hex string. For example, to specify
        // domain-name-servers you could do this:
        // {
        //     "name": "domain-name-servers",
        //     "code": 6,
        //     "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, 192.0.2.2"
        },

        // Typically people prefer to refer to options by their names, so they
        // don't need to remember the code names. However, some people like
        // to use numerical values. For example, option "domain-name" uses
        // option code 15, so you can reference to it either by
        // "name": "domain-name" or "code": 15.
        {
            "code": 15,
            "data": "chileshe.net"
        },

        // Domain search is also a popular option. It tells the client to
        // attempt to resolve names within those specified domains. For
        // example, name "foo" would be attempted to be resolved as
        // foo.mydomain.example.com and if it fails, then as foo.example.com
        {
            "name": "domain-search",
            "data": "chileshe.net"
        },
```

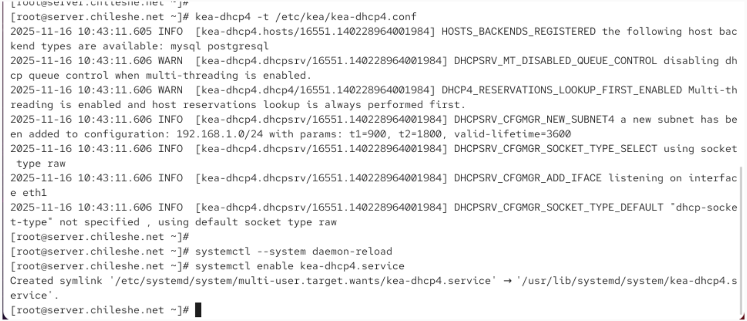
Настройка подсети



```
    //    }
    // ],

    // Below an example of a simple IPv4 subnet declaration. Uncomment to enable
    // it. This is a list, denoted with [ ], of structures, each denoted with
    // { }. Each structure describes a single subnet and may have several
    // parameters. One of those parameters is "pools" that is also a list of
    // structures.
    "subnet4": [
        {

            "id": 1,

            "subnet": "192.168.1.0/24",

            "pools": [ { "pool": "192.168.1.30 - 192.168.1.199" } ],

            "option-data": [
                {
                    // For each IPv4 subnet you most likely need to specify at
                    // least one router.
                    "name": "routers",
                    "data": "192.168.1.1"
                }
            ]

            // You can add more subnets there.
        }
    ],

```

Рис. 3: Настройка подсети DHCP

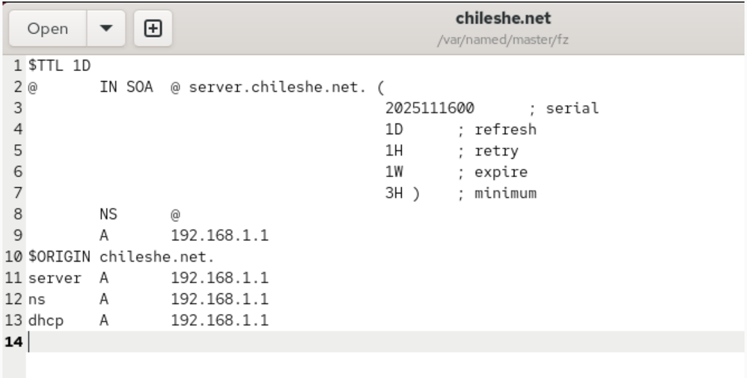
Проверка конфигурации



```
[root@server.chileshe.net ~]#
[root@server.chileshe.net ~]# kea-dhcp4 -t /etc/kea/kea-dhcp4.conf
2025-11-16 10:43:11.605 INFO  [kea-dhcp4.hosts/16551.140228964001984] HOSTS_BACKENDS_REGISTERED the following host bac
kend types are available: mysql postgresql
2025-11-16 10:43:11.606 WARN  [kea-dhcp4.dhcpsrv/16551.140228964001984] DHCPSRV_MT_DISABLED_QUEUE_CONTROL disabling dh
cp queue control when multi-threading is enabled.
2025-11-16 10:43:11.606 WARN  [kea-dhcp4.dhcp4/16551.140228964001984] DHCP4_RESERVATIONS_LOOKUP_FIRST_ENABLED Multi-th
reading is enabled and host reservations lookup is always performed first.
2025-11-16 10:43:11.606 INFO  [kea-dhcp4.dhcpsrv/16551.140228964001984] 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
2025-11-16 10:43:11.606 INFO  [kea-dhcp4.dhcpsrv/16551.140228964001984] DHCPSRV_CFGMGR_SOCKET_TYPE_SELECT using socket
 type raw
2025-11-16 10:43:11.606 INFO  [kea-dhcp4.dhcpsrv/16551.140228964001984] DHCPSRV_CFGMGR_ADD_IFACE listening on interfac
e eth1
2025-11-16 10:43:11.606 INFO  [kea-dhcp4.dhcpsrv/16551.140228964001984] DHCPSRV_CFGMGR_SOCKET_TYPE_DEFAULT "dhcp-socke
t-type" not specified , using default socket type raw
[root@server.chileshe.net ~]#
[root@server.chileshe.net ~]# systemctl --system daemon-reload
[root@server.chileshe.net ~]# 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.chileshe.net ~]# █
```

Рис. 4: Проверка Kea

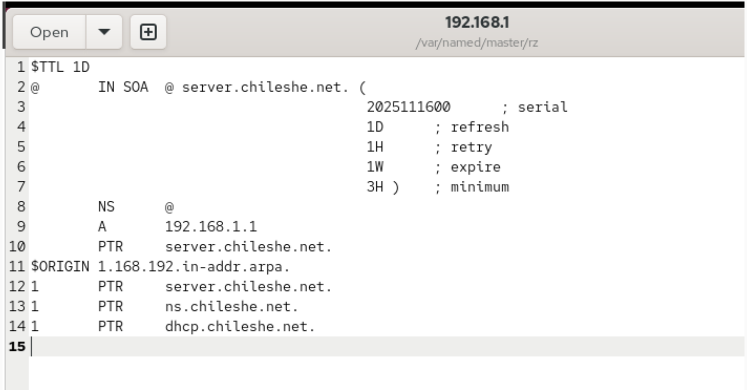
Настройка прямой DNS-зоны



```
$TTL 1D
@       IN SOA  @ server.chileshe.net. (
                                        2025111600      ; serial
                                        1D      ; refresh
                                        1H      ; retry
                                        1W      ; expire
                                        3H )    ; minimum
        NS      @
        A       192.168.1.1
$ORIGIN chileshe.net.
server  A       192.168.1.1
ns      A       192.168.1.1
dhcp    A       192.168.1.1

```

Рис. 5: Прямая зона

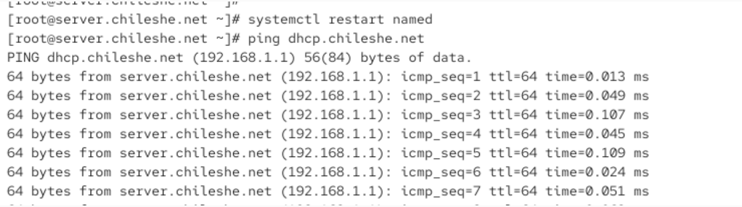
Настройка обратной DNS-зоны



```
$TTL 1D
@       IN SOA  @ server.chileshe.net. (
                                        2025111600      ; serial
                                        1D      ; refresh
                                        1H      ; retry
                                        1W      ; expire
                                        3H )    ; minimum
        NS      @
        A       192.168.1.1
        PTR     server.chileshe.net.
$ORIGIN 1.168.192.in-addr.arpa.
1       PTR     server.chileshe.net.
1       PTR     ns.chileshe.net.
1       PTR     dhcp.chileshe.net.
```

Рис. 6: Обратная зона

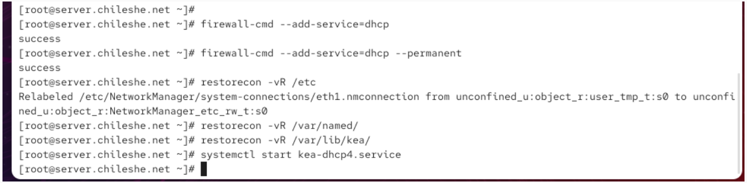
Проверка разрешения имён



```
[root@server.chileshe.net ~]#
[root@server.chileshe.net ~]# systemctl restart named
[root@server.chileshe.net ~]# ping dhcp.chileshe.net
PING dhcp.chileshe.net (192.168.1.1) 56(84) bytes of data.
64 bytes from server.chileshe.net (192.168.1.1): icmp_seq=1 ttl=64 time=0.013 ms
64 bytes from server.chileshe.net (192.168.1.1): icmp_seq=2 ttl=64 time=0.049 ms
64 bytes from server.chileshe.net (192.168.1.1): icmp_seq=3 ttl=64 time=0.107 ms
64 bytes from server.chileshe.net (192.168.1.1): icmp_seq=4 ttl=64 time=0.045 ms
64 bytes from server.chileshe.net (192.168.1.1): icmp_seq=5 ttl=64 time=0.109 ms
64 bytes from server.chileshe.net (192.168.1.1): icmp_seq=6 ttl=64 time=0.024 ms
64 bytes from server.chileshe.net (192.168.1.1): icmp_seq=7 ttl=64 time=0.051 ms
```

Рис. 7: Проверка DNS

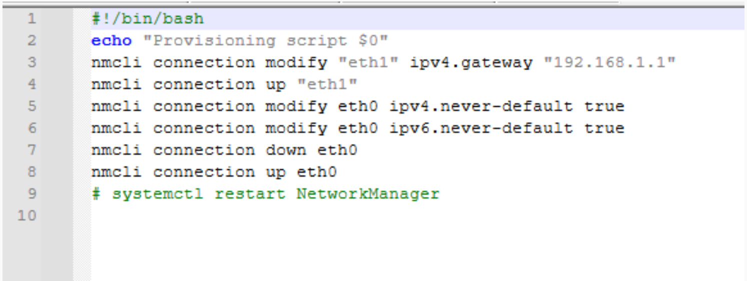
Настройка firewall и SELinux



```
[root@server.chileshe.net ~]#
[root@server.chileshe.net ~]# firewall-cmd --add-service=dhcp
success
[root@server.chileshe.net ~]# firewall-cmd --add-service=dhcp --permanent
success
[root@server.chileshe.net ~]# restorecon -vR /etc
Relabeled /etc/NetworkManager/system-connections/eth1.nmconnection from unconfined_u:object_r:user_tmp_t:s0 to unconfi
ned_u:object_r:NetworkManager_etc_rw_t:s0
[root@server.chileshe.net ~]# restorecon -vR /var/named/
[root@server.chileshe.net ~]# restorecon -vR /var/lib/kea/
[root@server.chileshe.net ~]# systemctl start kea-dhcp4.service
[root@server.chileshe.net ~]#
```

Рис. 8: Firewall и SELinux

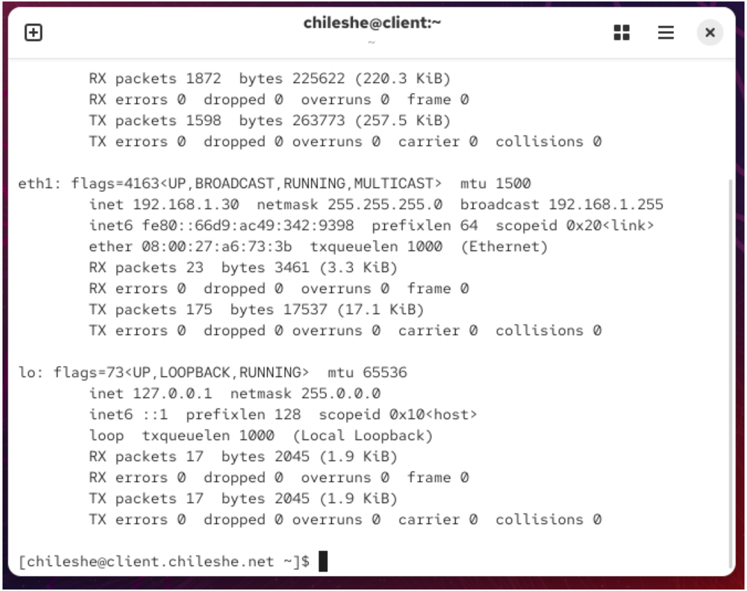
Скрипт маршрутизации клиента



```
#!/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
```

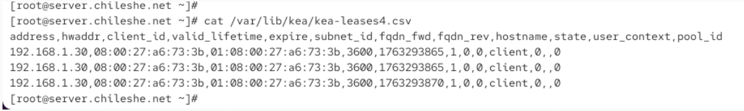
Рис. 9: Скрипт маршрутизации

Интерфейсы клиента



```
        RX packets 1872  bytes 225622 (220.3 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 1598  bytes 263773 (257.5 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::66d9:ac49:342:9398  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:a6:73:3b  txqueuelen 1000  (Ethernet)
        RX packets 23  bytes 3461 (3.3 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 175  bytes 17537 (17.1 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 17  bytes 2045 (1.9 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 17  bytes 2045 (1.9 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

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

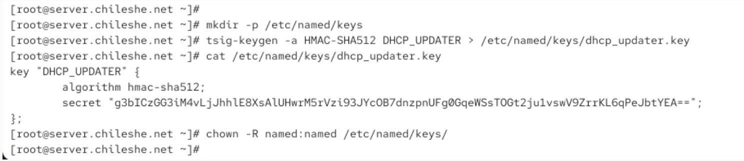
Анализ DHCP-аренд



```
[root@server.chileshe.net ~]#
[root@server.chileshe.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:a6:73:3b,01:08:00:27:a6:73:3b,3600,1763293865,1,0,0,client,0,,0
192.168.1.30,08:00:27:a6:73:3b,01:08:00:27:a6:73:3b,3600,1763293865,1,0,0,client,0,,0
192.168.1.30,08:00:27:a6:73:3b,01:08:00:27:a6:73:3b,3600,1763293870,1,0,0,client,0,,0
[root@server.chileshe.net ~]#
```

Рис. 11: kea-leases4.csv

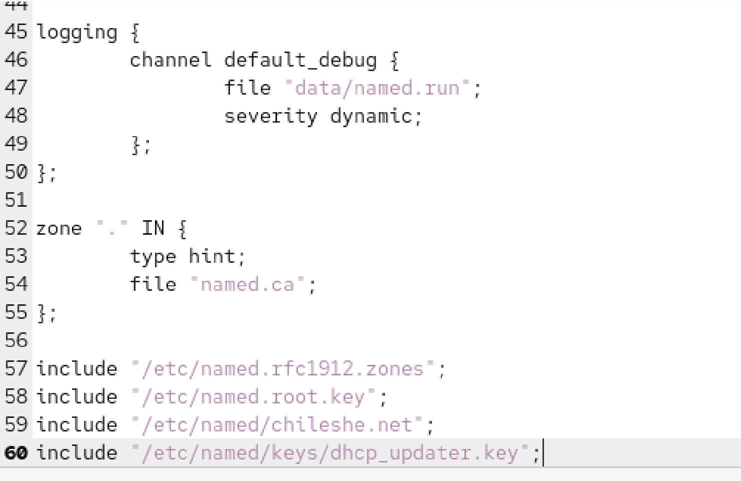
Генерация TSIG-ключа



```
[root@server.chileshe.net ~]#
[root@server.chileshe.net ~]# mkdir -p /etc/named/keys
[root@server.chileshe.net ~]# tsig-keygen -a HMAC-SHA512 DHCP_UPDATER > /etc/named/keys/dhcp_updater.key
[root@server.chileshe.net ~]# cat /etc/named/keys/dhcp_updater.key
key "DHCP_UPDATER" {
        algorithm hmac-sha512;
        secret "g3bICzGG3iM4vLjJhhlE8XsAlUHwrM5rVzi93JYcOB7dnzpnUFg0GqeWSsTOGt2ju1vswV9ZrrKL6qPeJbtYEA==";
};
[root@server.chileshe.net ~]# chown -R named:named /etc/named/keys/
[root@server.chileshe.net ~]#
```

Рис. 12: TSIG-ключ

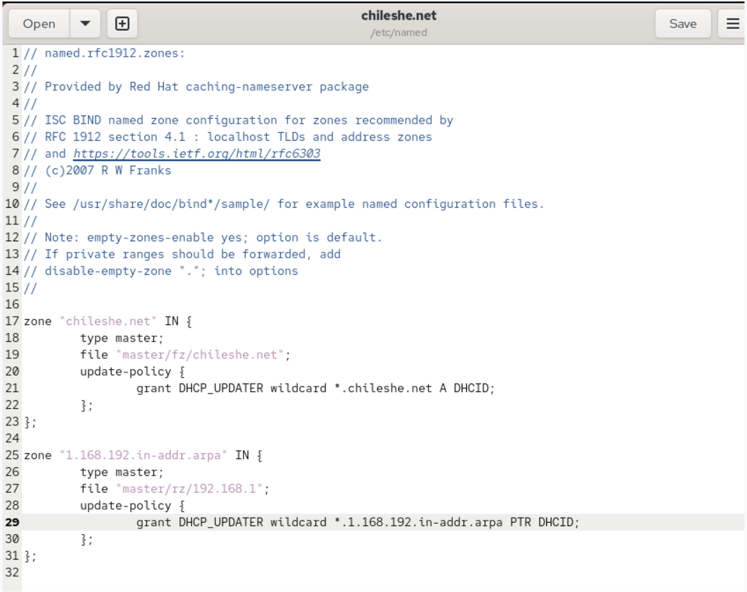
Подключение ключа в named



```
logging {
        channel default_debug {
                file "data/named.run";
                severity dynamic;
        };
};

zone "." IN {
        type hint;
        file "named.ca";
};

include "/etc/named.rfc1912.zones";
include "/etc/named.root.key";
include "/etc/named/chileshe.net";
include "/etc/named/keys/dhcp_updater.key";
```

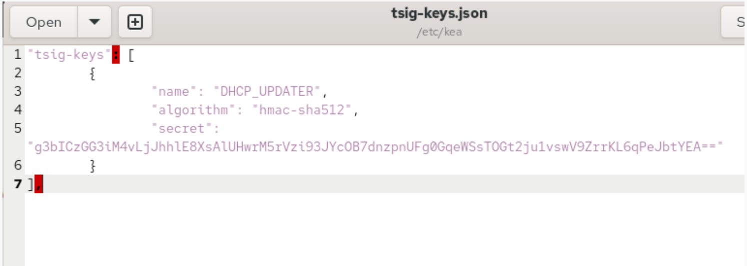
Рис. 13: Вставка ключа

Настройка политики обновлений прямой зоны



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

```

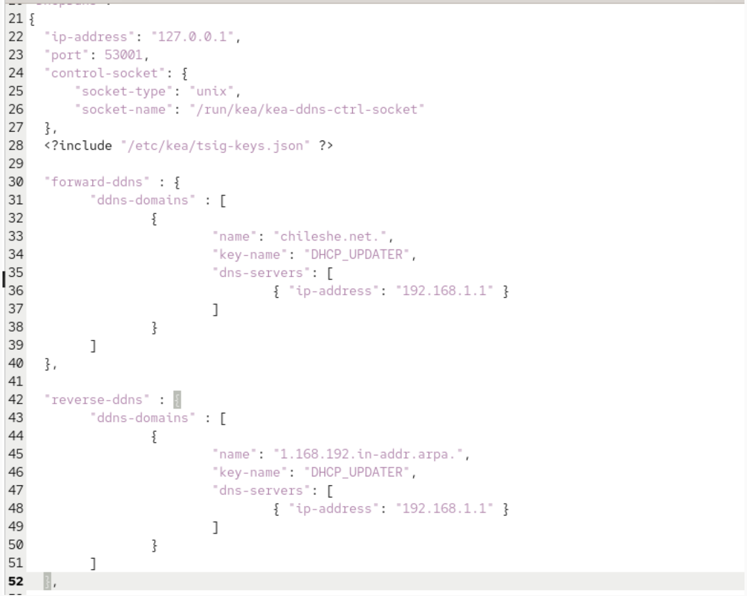
Настройка политики обновлений обратной зоны



```
"tsig-keys": [
        {
                "name": "DHCP_UPDATER",
                "algorithm": "hmac-sha512",
                "secret":
"g3bICzGG3iM4vLjJhhlE8XsAlUHwrM5rVzi93JYcOB7dnzpnUFg0GqeWSsTOGt2ju1vswV9ZrrKL6qPeJbtYEA=="
        }
],
```

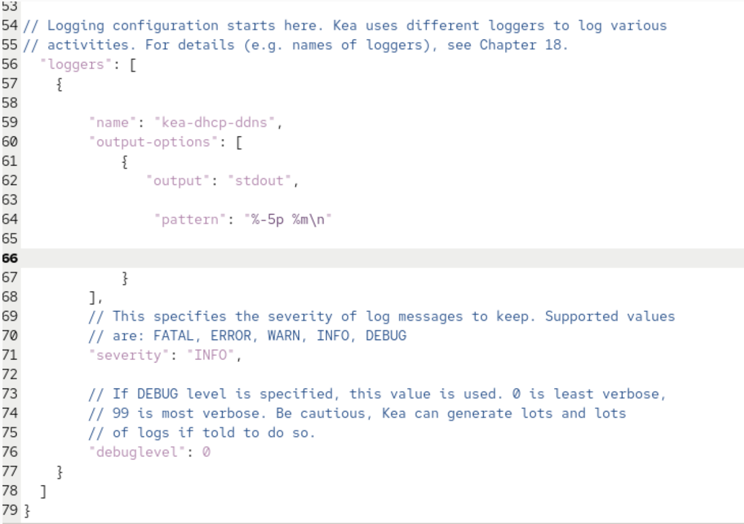
Рис. 15: update-policy RZ

Конфигурация tsig-keys.json



```
{
  "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": "chileshe.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" }
                        ]
                }
        ]
  },
```

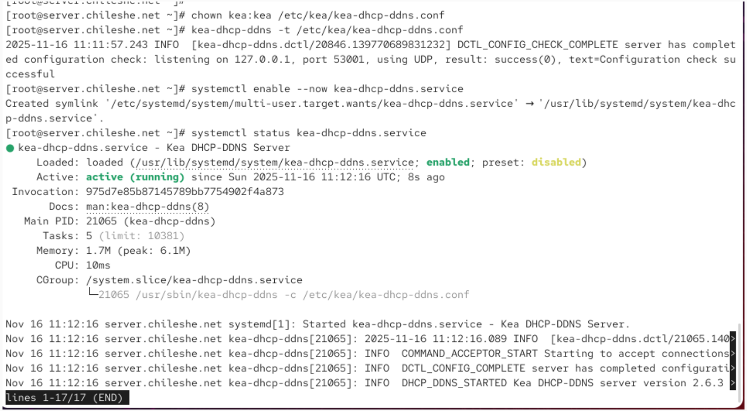
Конфигурация Kea DHCP-DDNS



```
// Logging configuration starts here. Kea uses different loggers to log various
// activities. For details (e.g. names of loggers), see Chapter 18.
  "loggers": [
    {

        "name": "kea-dhcp-ddns",
        "output-options": [
            {
               "output": "stdout",

                "pattern": "%-5p %m\n"


            }
        ],
        // This specifies the severity of log messages to keep. Supported values
        // are: FATAL, ERROR, WARN, INFO, DEBUG
        "severity": "INFO",

        // If DEBUG level is specified, this value is used. 0 is least verbose,
        // 99 is most verbose. Be cautious, Kea can generate lots and lots
        // of logs if told to do so.
        "debuglevel": 0
    }
  ]
}
```

Рис. 17: kea-dhcp-ddns.conf

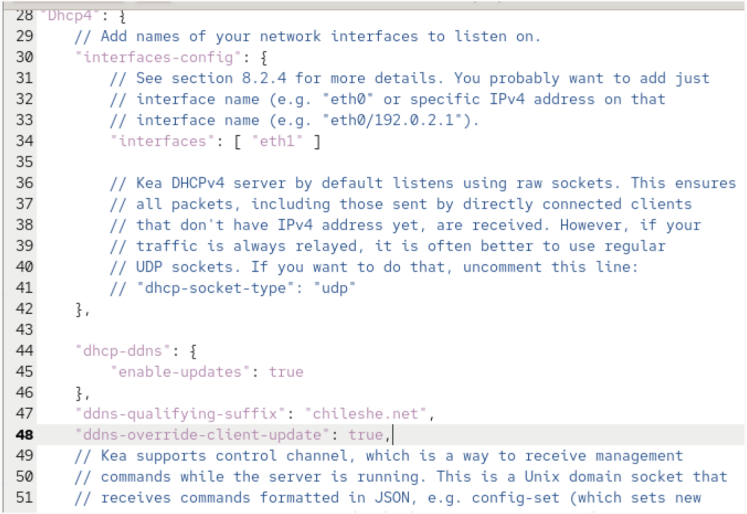
Статус Kea DDNS



```
[root@server.chileshe.net ~]#
[root@server.chileshe.net ~]# chown kea:kea /etc/kea/kea-dhcp-ddns.conf
[root@server.chileshe.net ~]# kea-dhcp-ddns -t /etc/kea/kea-dhcp-ddns.conf
2025-11-16 11:11:57.243 INFO  [kea-dhcp-ddns.dctl/20846.139770689831232] 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.chileshe.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-dhc
p-ddns.service'.
[root@server.chileshe.net ~]# 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 Sun 2025-11-16 11:12:16 UTC; 8s ago
 Invocation: 975d7e85b87145789bb7754902f4a873
       Docs: man:kea-dhcp-ddns(8)
   Main PID: 21065 (kea-dhcp-ddns)
      Tasks: 5 (limit: 10381)
     Memory: 1.7M (peak: 6.1M)
        CPU: 10ms
     CGroup: /system.slice/kea-dhcp-ddns.service
             └─21065 /usr/sbin/kea-dhcp-ddns -c /etc/kea/kea-dhcp-ddns.conf

Nov 16 11:12:16 server.chileshe.net systemd[1]: Started kea-dhcp-ddns.service - Kea DHCP-DDNS Server.
Nov 16 11:12:16 server.chileshe.net kea-dhcp-ddns[21065]: 2025-11-16 11:12:16.089 INFO  [kea-dhcp-ddns.dctl/21065.140>
Nov 16 11:12:16 server.chileshe.net kea-dhcp-ddns[21065]: INFO  COMMAND_ACCEPTOR_START Starting to accept connections>
Nov 16 11:12:16 server.chileshe.net kea-dhcp-ddns[21065]: INFO  DCTL_CONFIG_COMPLETE server has completed configurati>
Nov 16 11:12:16 server.chileshe.net kea-dhcp-ddns[21065]: INFO  DHCP_DDNS_STARTED Kea DHCP-DDNS server version 2.6.3 >
lines 1-17/17 (END)
```

Рис. 18: Kea DDNS status

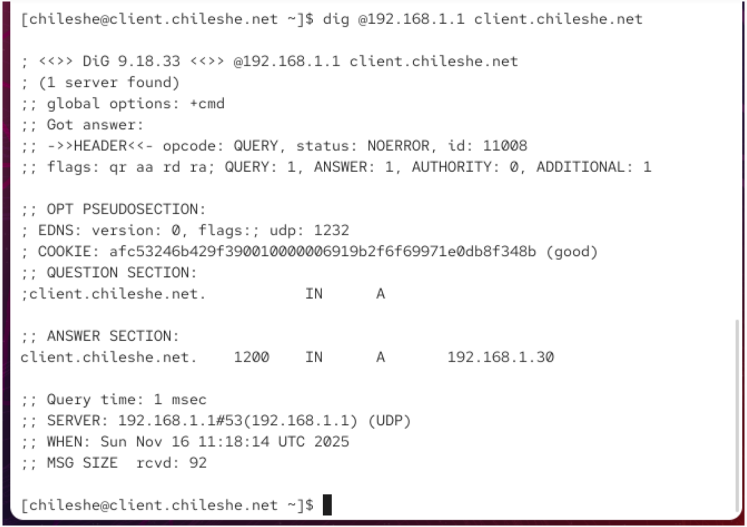
Обновления DDNS в DHCP



```
"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": "chileshe.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
```

Рис. 19: dhcp4 DDNS параметры

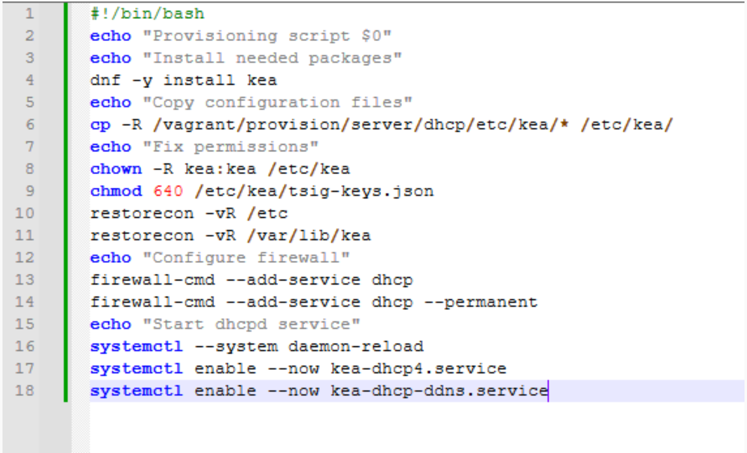
Проверка DDNS через dig



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

; <<>> DiG 9.18.33 <<>> @192.168.1.1 client.chileshe.net
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 11008
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: afc53246b429f390010000006919b2f6f69971e0db8f348b (good)
;; QUESTION SECTION:
;client.chileshe.net.           IN      A

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

;; Query time: 1 msec
;; SERVER: 192.168.1.1#53(192.168.1.1) (UDP)
;; WHEN: Sun Nov 16 11:18:14 UTC 2025
;; MSG SIZE  rcvd: 92

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

Рис. 20: dig результат

Завершение настройки



```bash
#!/bin/bash
echo "Provisioning script $0"
echo "Install needed packages"
dnf -y install kea
echo "Copy configuration files"
cp -R /vagrant/provision/server/dhcp/etc/kea/* /etc/kea/
echo "Fix permissions"
chown -R kea:kea /etc/kea
chmod 640 /etc/kea/tsig-keys.json
restorecon -vR /etc
restorecon -vR /var/lib/kea
echo "Configure firewall"
firewall-cmd --add-service dhcp
firewall-cmd --add-service dhcp --permanent
echo "Start dhcpd service"
systemctl --system daemon-reload
systemctl enable --now kea-dhcp4.service
systemctl enable --now kea-dhcp-ddns.service
```

Рис. 21: dhcp.sh

Итоги работы

Вывод

Настроен DHCP-сервер Kea, интегрированный с Bind9 через TSIG-ключи. Динамические обновления DNS функционируют корректно: клиенты автоматически получают IP-адреса, а соответствующие A- и PTR-записи создаются в DNS-зонах. Инфраструктура полностью автоматизирована и прошла успешное тестирование.