Настройка связки DNS+DHCP_UPDATER

Опубликовано muff в Вс, 2010-09-05 21:42

Решил настроить динамическое обновление ДНС по событию - то есть, при выдаче IP-адреса, DHCP будет автоматически добавлять запись в DNS, обновляя как "прямую" так и "обратную" зону. Будем отталкиваться от того, что уже есть настроенные и рабочие сервисы DNS [1] и DHCP [2],

Исходные данные следующие:

- **домен:** office.local
- **IP-адресация:** 192.168.100.0/24

Первый шаг - это генерация ключа обновлений. Поскольку используем BIND версии 9, то команда будет следующей:

```
# dnssec-keygen -a HMAC-MD5 -b 128 -n USER DHCP_UPDATER
Kdhcp_updater.+157+54483
```

(если установлен BIND версии 8, то необходимо воспользоваться командой **dnskeygen -H 128 -u -c -n DHCP_UPDATER**)

Посмотрим на результат команды:

```
# cat Kdhcp_updater.+157+54483.key
DHCP_UPDATER. IN KEY 0 3 157 evUUzuAFS+xk0178ftrS1g==
```

Приступаем к редактированию **dhcpd.conf**. Листинг конфигурационного файла до редактирования:

```
# cat /usr/local/etc/dhcpd.conf
option domain-name "office.local";
default-lease-time 304400;
max-lease-time 604800;
authoritative;
ddns-update-style none;
subnet 192.168.100.0 netmask 255.255.255.0 {
range 192.168.100.1 192.168.100.50;
option domain-name-servers 192.168.100.55;
option routers 192.168.100.55; }
```

Вставляем в dhcpd.conf следующие блоки:

```
ddns-updates on;
ddns-update-style interim;
ddns-domainname "office.local";
ddns-rev-domainname "100.168.192.in-addr.arpa";
ignore client-updates;
update-static-leases true;

key DHCP_UPDATER {
        algorithm hmac-md5;
        secret evUUzuAFS+xk0178ftrS1g==;
        }

zone office.local. {
```

```
        primary 127.0.0.1;
        key DHCP_UPDATER;
        }

zone 192.168.192.in-addr.arpa.{
        primary 127.0.0.1;
        key DHCP_UPDATER;
        }
```

В результате должно получиться:

```
# cat /usr/local/etc/dhcpd.conf
option domain-name "office.local";
default-lease-time 304400;
max-lease-time 604800;
authoritative;
ddns-updates on;
ddns-update-style interim;
ddns-domainname "office.local";
ddns-rev-domainname "100.168.192.in-addr.arpa";
ignore client-updates;
update-static-leases true;

key DHCP_UPDATER {
        algorithm hmac-md5;
        secret evUUzuAFS+xk0178ftrS1g==;
        }

zone office.local. {
        primary 127.0.0.1;
        key DHCP_UPDATER;
        }

zone 100.168.192.in-addr.arpa.{
        primary 127.0.0.1;
        key DHCP_UPDATER;
        }
  subnet 192.168.100.0 netmask 255.255.255.0 {
range 192.168.100.1 192.168.100.50;
option domain-name-servers 192.168.100.55;
option routers 192.168.100.55; }
```

Для того, чтобы изменения вступили в силу, перестартовываем DHCP:

```
# sh /usr/local/etc/rc.d/isc-dhcpd restart
Stopping dhcpd.
Starting dhcpd.
Internet Systems Consortium DHCP Server V3.0.7
Copyright 2004-2008 Internet Systems Consortium.
All rights reserved.
For info, please visit http://www.isc.org/sw/dhcp/ [3]
WARNING: Host declarations are global.  They are not limited to the scope you declared them in.
Wrote 0 deleted host decls to leases file.
Wrote 0 new dynamic host decls to leases file.
Wrote 49 leases to leases file.
Listening on BPF/vr0/00:13:46:64:1d:13/192.168.100/24
Sending on   BPF/vr0/00:13:46:64:1d:13/192.168.100/24
```

```
Sending on   Socket/fallback/fallback-net
```

Приступаем к DNS. Необходимо отредактировать **named.conf**, внеся в него описания зон **office.local**, **100.168.192.in-addr.arpa** и ключ **DHCP_UPDATER**, тоесть следующий блок:

```
key DHCP_UPDATER {
      algorithm hmac-md5;
      secret evUUzuAFS+xk0178ftrS1g==;
      };

zone "office.local" {
      type master;
      file "/dynamic/office.local";
      allow-update { key DHCP_UPDATER; };
      notify no;
};

zone "100.168.192.in-addr.arpa" {
      type master;
      file "/dynamic/100.168.192.in-addr.arpa";
      allow-update { key DHCP_UPDATER; };
      notify no;
};
```

Создадим каталог dynamic, где будут лежать файлы динамически обновляемых зон:

```
# mkdir /var/named/dynamic
```

Создаем файл **office.local** (прямая зона) следующего содержимого:

```
# cat /var/named/dynamic/office.local
$TTL 86400      ; 1 day@                  IN SOA  ns.office.local. admin.muff.kiev.u
a. (                                  2010090600 ; serial
   14400      ; refresh (4 hours)                                7200       ; retry
(2 hours)                                    3600000    ; expire (5 weeks 6 days 16 hour
s)                                  86400      ; minimum (1 day)
          )                          NS      ns.office.local.ns                    A
       192.168.100.55
```

Создаем файл обратной зоны **100.168.192.in-addr.arpa**:

```
# cat /var/named/dynamic/100.168.192.in-addr.arpa
$TTL 86400      ; 1 day@                  IN SOA  ns.office.local. admin.muff.kiev.u
a. (                                  2010090600 ; serial
   14400      ; refresh (4 hours)                                7200       ; retry
(2 hours)                                    3600000    ; expire (5 weeks 6 days 16 hour
s)                                  86400      ; minimum (1 day)
          )                          NS        ns.office.local.55.100.168.192
 PTR       ns.office.local.
```

Для того, чтобы named имел право записи в файлы, сделаем его рекурсивно владельцем каталога:

```
# chown -R bind:bind /var/named/dynamic/
```

Перезапускаем named:

```
# rndc reload
server reload successful
```

DNS-сервер готов к обновлениям. Для того, чтобы проверить это, создадим файл следующего содержания:

```
# cat testdns.txt
key DHCP_UPDATER evUUzuAFS+xk0178ftrS1g==
zone office.local
update add virtual 86400 A 192.168.100.200
send
zone 100.168.192.in-addr.arpa
update add 200 86400 PTR test.office.local.
send
```

Следующей командой проверяем, все ли нормально отрабатывается:

```
# nsupdate -d testdns.txt
```

Команда должна завершиться без ошибок, а в каталоге dynamic должны появиться файлы с расширением jnl:

```
# ls -la /var/named/dynamic/
total 16drwxr-xr-x  2 bind  bind   512  6 ??? 01:24 .drwxr-xr-x  7 root  wheel  512
 3 ??? 01:21 ..-rw-r--r--  1 bind  bind   485  6 ??? 01:24 100.168.192.in-addr.arpa-
rw-r--r--  1 bind  bind   800  6 ??? 01:23 100.168.192.in-addr.arpa.jnl-rw-r--r--  1
 bind  bind   509  6 ??? 01:24 office.local-rw-r--r--  1 bind  bind   817  6 ??? 01:
23 office.local.jnl
```

?? ???? ?????? DNS ? DHCP ????? ??????? ??????????. ??????? ????, ????? ??????? ???????????????, ??????? ????, ? ?????????, ??? DNS-??????? ????? ??????????? ??? ? ??????, ??? ? ? ???????? ????.

Источник (получено *2026-11-12 05:58*):
http://muff.kiev.ua/content/nastroika-svyazki-dnsdhcpupdater

Ссылки:
[1] http://muff.kiev.ua/content/bind-9-nastroika-dns-servera
[2] http://muff.kiev.ua/content/dhcp-server-v-seti-esli-neokhota-begat-ot-kompyutera-k-kompyuteru
[3] http://www.isc.org/sw/dhcp/