DHCP und dynamischer Update eines DNS

Als Voraussetzung für diese Dokumentation wird eine funktionierende Konfiguration eines DNS Servers, mit den entsprechenden Zonefiles angenommen.

Die hier verwendete Domain soll in-put.local heissen, der Name- und DHCP Server laufen auf der IP-Adresse 192.168.0.12, als externer DNS wird die IP-Adresse 195.243.130.10 verwendet.

Der DHCP-Server sollte mehrere IP-Adressbereiche verwalten und die Clients, welche eine IP-Adresse von ihm bekamen, in den DNS eintragen.

Zur Sicherheit soll nicht jeder DHCP-Server in der Lage sein, Informationen über die IP-Adressen und die zugehörigen Rechnernamen an den Nameserver zu übertragen. Daher erfolgt eine Authentifizierung des DHCP-Servers am Nameserver. Der erforderliche Schlüssel wird mit dem Programm *dnssec-keygen* erzeugt, daß zum Nameserver BIND9 gehört.

```
cd /etc
dnssec-keygen -a HMAC-MD5 -b 128 -n USER DHCP_UPDATER
```

-a Algorithmus, hier HMAC-MD5
-b Laenge des Keys, hier 128 Bit
-n Nametype, hier USER (namens) DHCP_UPDATER

Im Verzeichniss /etc sind nun zwei neue Dateien entstanden:

```
Kdhcp_updater.+157+32388.key
Kdhcp_updater.+157+32388.private
```

Das .key File enthält den DNS KEY Record, der direkt oder mit einem $INCLUDE Statement in ein Zonefile übernommen werden kann und das .private File, welches algorithmusspezifische Angaben enthält, die keine generellen Leserechte, sondern ausschließlich für den Administrator (chmod 600 root) haben sollten.

```
cat Kdhcp_updater.+157+32388.private

    Private-key-format: v1.2
    Algorithm: 157 (HMAC_MD5)
    Key: dZyOvL+WTQP7BYQEgaNqRg==
```

Der Schlüssel der hinter Key: steht wird nun als Schlüssel für den DHCP-Server und für den DNS-Server benutzt. Die Konfiguration des DHCP Servers erfolgt über die Datei /etc/dhcpd.conf

```
# Dynamischer Update DNS, verwende sicheres Schema. Die Updates werden in temporäre Dateien
# (*.jnl) gespeichert und dann erst in die Zonendateien übertragen.
ddns-update-style interim;
```

```
# Dynamischer Update DNS, Name der Domain
ddns-domainname "in-put.de";

# Dynamischer Update DNS, statische Adressen auch im DNS updaten
update-static-leases true;

# Festlegen des KEY, secret = Schlüssel von dnssec-keygen
# Welche Zonen sollen aktualisiert werden
key DHCP_UPDATER {
        algorithm HMAC-MD5.SIG-ALG.REG.INT;
        secret dZyOvL+WTQP7BYQEgaNqRg==;
        }

zone in-put.de.
        {
        primary 192.168.0.12;
        key DHCP_UPDATER;
        }

zone 0.168.192.in-addr.arpa.
        {
        primary 192.168.0.12;
        key DHCP_UPDATER;
        }

# this subnet is served by us
    authoritative;

    # declare the lease times (the time after which a client will renew its lease)
    default-lease-time 86400;
    max-lease-time 86400;

    # dynamischer Adressbereich
    subnet 192.168.0.0 netmask 255.255.255.0
        {
        option broadcast-address 192.168.0.255;
        option subnet-mask 255.255.255.0;
        option routers 192.168.0.1;
        option domain-name-servers 195.243.130.10;
        range 192.168.0.224 192.168.0.230;

        # Feste Adressen, hier Drucker
        host xerox
            {
                hardware ethernet 00:00:AA:77:B0:2A;
                fixed-address 192.168.0.13;
                }
        }
```

Nun zu den Einträgen in der /etc/named.conf

```
options
    {
```

```
        auth-nxdomain yes;
        directory "/var/named";
        forwarders { 195.243.130.10; 194.25.2.129; };

        #forward first;
        listen-on { any; };

        cleaning-interval 120;
};
# Mit den folgenden Logging-Einträgen erhält man in der /var/log/messages die Nachrichten des
# Nameservers angezeigt, wenn der DHCP die Informationen an den BIND9 sendet
logging {
      # Log queries to a file limited to a size of 100 MB.
      channel query_logging {
            file "/var/log/named_querylog";
            versions 3 size 100M;
            print-time yes;               // timestamp log entries
            };
      category queries {
            query_logging;
            };

      # Or log this kind alternatively to syslog.
            channel syslog_queries {
            syslog user;
            severity info;
            };

      category queries { syslog_queries; };

      # Log general name server errors to syslog.
      channel syslog_errors {
            syslog user;
            severity error;
            };

      category default { syslog_errors;  };

      # Don't log lame server messages.
      category lame-servers { null; };
            };
};

zone "localhost" in {
        type master;
        file "localhost.zone";
};

zone "0.0.127.in-addr.arpa" in {
        type master;
        file "127.0.0.zone";
};

zone "." in {
```

```
        type hint;
        file "root.hint";
};

key DHCP_UPDATER {
        algorithm HMAC-MD5.SIG-ALG.REG.INT;
        secret dZyOvL+WTQP7BYQEgaNqRg==;
    };

zone "0.168.192.in-addr.arpa" {
        type master;
        file "0.168.192.in-addr.arpa";
        allow-update { key DHCP_UPDATER; };
        notify yes;
};

zone "in-put.de" {
        type master;
        file "in-put.de";
        allow-update { key DHCP_UPDATER; };
        notify yes;
};
```

Unter SuSE müssen Sie in der Datei */etc/sysconfig/dhcpd* die folgende Variable setzen:

```
DHCPD_INTERFACE=""
```

Tragen Sie dort das Interface (z.B. eth0) ein, auf dem der DHCP-Server auf Anfragen warten soll.
Wenn nun in den beiden Dateien keine Tippfehler, vergessene Semikolone, oder so zu finden sind, sollten sich die beiden Dienste, DHCP und DNS über die jeweiligen Start- und Stop Skripte neu starten lassen; also:

```
/etc/init.d/dhcpd restart
/etc/init.d/named restart
```

Sollten sich doch Fehler in die Konfigurationsdateien eingeschlichen haben werden diese, mit Angabe der Zeilennummer beim Starten der Dienste bemerkbar machen. Andernfalls sind die Ausgaben der Dienste in der Datei /var/log/messages zu finden.

Achtung: RedHat, SuSE und Windowsübergeben beim „Anmelden“ beim DHCP Server ihren Hostnamen an denselben.Um dies bei Debian zu erreichen muss in der /etc/dhclient.conf die Option „send host-name „name des rechners“ auskommentiert werden.

Ein weiterer Stolperstein sind die Rechte am Verzeichnis /var/named. Für dieses Verzeichnis besitzt nur root Schreibrechte. Der Nameserver läuft aber zumeist unter der UID named. Daher muß der Eigentümer am

Verzeichnis mit dem Befehl *chown named /var/named* entsprechend gesetzt werden, sonst kann der Nameserver die Aktualisierungen durch den DHCP-Server nicht speichern.

Hinweis:
Bei manchen Distributionen/Versionen befinden sich die Zonendateien nicht unter */var/named*, sondern unter */var/lib/named*.

Soll der DHCP-Server zwei Netzwerke bedienen, z.B. 192.168.0.0/24 (siehe oben) und 10.10.10.0/24, so sind folgende Änderungen vorzunehmen:

/etc/sysconfig/dhcpd:

```
DHCPD_INTERFACE="eth0 eth1"
```

/etc/dhcpd.conf:

```
zone 10.10.10.in-addr.arpa.
{
        primary 192.168.0.103;
        key DHCP_UPDATER;
}

subnet 10.10.10.0 netmask 255.255.255.0
{
        option broadcast-address 10.10.10.255;
        option subnet-mask 255.255.255.0;
        option routers 10.10.10.1;
        option domain-name-servers 195.243.130.10;
        range 10.10.10.100 10.10.10.254;
}
```

/etc/named.conf:

```
zone "10.10.10.in-addr.arpa" in {
        type master;
        file "10.10.10.IN-ADDR.ARPA.zone";
        allow-update { key DHCP_UPDATER;};
        notify yes;
};
```

Zudem ist in */var/lib/named* bzw. */var/named* die Zonendatei für eine Reverse Lookup von 10.10.10.0 anzulegen.