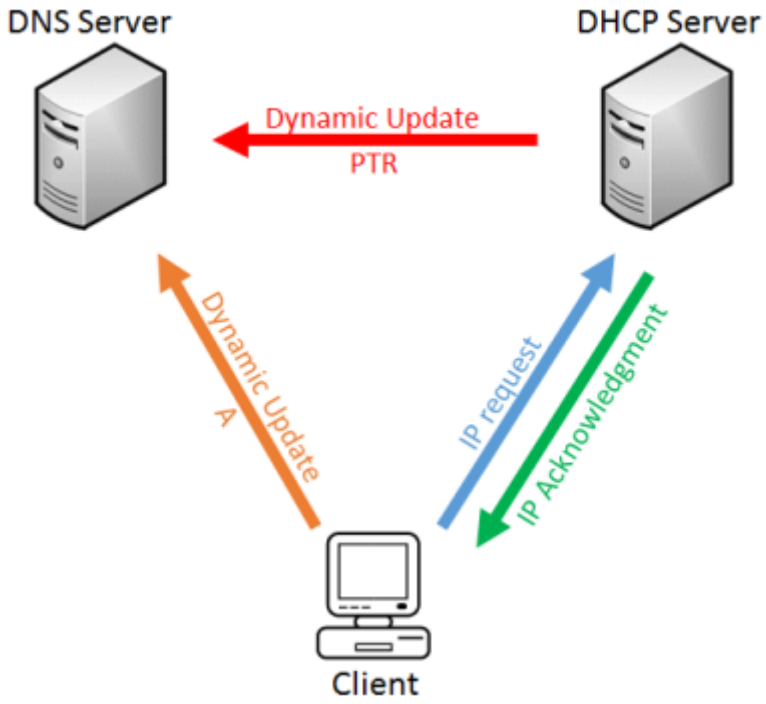
DNS / DHCP und DDNS mit Debian

Hier wird beschrieben, wie im ersten Schritt ein grundlegender **DNS Server** mit **zwei unterschiedlichen Zonen** *(über zwei Netzen)* konfiguriert werden kann. Darauf folgend konfigurieren wir einen **ISC-DHCP Server**, der die IP-Adressierung im **LAN** Netzwerk übernimmt. Zum Schluss, wird noch das Zusammenspiel von DNS und DPCP Server via einer verschlüsselten RNDC-Verbindung realisiert. Dieses Konstrukt, nennt sich dann DDNS.



Beim **DDNS** können dann automatisiert DHCP Clients vom ISC-DHCP-Server in die DNS Zonen eingetragen werden und so das Netz dynamisch verwaltet werden.

Standalone DNS Server

Die nachfolgenden Installationen, werden alle mit dem Benutzer **root** durchgeführt. Deshalb wird als ersten Schritt einmal auf das frisch installierte **Debian / Ubuntu** per **Putty** verbunden und Authentifiziert.

Anschliessend wird das System erstmals auf den neusten Stand gebracht und das bind9, welches unseren DNS-Server repräsentiert installiert:

```
# apt-get update
# apt-get –y upgrade

# apt-get -y install bind9 bind9utils dnsutils
```

Wichtig! Nicht vergessen dem DNS-Server eine **fixe IP Adresse** in der '/etc/network/interfaces' zuzuweisen. Hierbei wird beachtet, dass der Eintrag: **dns-nameservers 127.0.0.1** zu setzen ist!

- **Netzwerk Konfiguration unter Debian / Ubuntu**

DNS-Server Konfiguration

Im Folgenden wird die Konfiguration von **bind9** Dokumentiert.

Auf dem Server haben wir nun mehrere Konfigurationsdateien:

- Die Datei **/etc/bind/named.conf**, *beinhaltet die Haupt-Incudes, von der aus dann weiteren config-files eingebunden werden.*
- Die **/etc/bind/named.conf.options** *beinhaltet verschiedenen Optionen zum DNS Server.*
- Die **/etc/bind/named.conf.default-zones** *beinhaltet die DNS lokalen Zonen, wie z.B. den localhost.*
- Im **/etc/bind/named.conf.local** *werden unsere eigenen späteren lokalen Zonen definieren!*

Definieren der lokalen Zonen

Im ersten Schritt, werden nun erstmals in der `named.conf.local` unsere lokalen Zonen definiert; damit zeigen wir auch gleich auf unsere nachehr zu erstellenden Zonen-Files

```
# vim /etc/bind/named.conf.local
```

```
# Konfigurationsfile /etc/bind/named.conf.local
# Definieren von unseren neuen Zonen.

    # LAN-NETWORK
    zone "blackgate.lan" in {
        type master;
        file "/var/lib/bind/db.blackgate.lan"; };

    zone "1.168.192.in-addr.arpa" in {
        type master;
        file "/var/lib/bind/db.192.168.1"; };

    # DMZ-NETWORK
    zone "blackgate.dmz" in {
            type master;
        file "/var/lib/bind/db.blackgate.dmz"; };
```

```
    zone "13.168.192.in-addr.arpa" in {
        type master;
        file "/var/lib/bind/db.192.168.13"; };
```

*Wie man sieht, erstellen wir unsere **Zonen Files** unter **/var/lib/bind**. Dies ist so, da später spätestens bei der Konfiguration von DDNS der DNS-Server auch selber in die Zonen-Files schreiben muss, und sich nur dort eine wirklich gute vertretbare Lösung dazu bietet.*

Erstellen der Zonen Files

Nun werden anhand des erstellen unserer Zonenfiles die Schranken für den DNS erstellt und ihm überhaupt auch gleich die Möglichkeit gegeben DNS-Queries aus dem LAN und der DMZ aufzulösen.

Erstellen der Forward-Zone für das LAN Netzwerk:

```
# vim /var/lib/bind/db.blackgate.lan
```

```
$TTL    604800
@   IN    SOA     (
            ns.blackgate.dmz.         ; MNAME Record
            admin.blackgate.dmz.         ; Mail von DNS Admin
            2017022001            ; Serial
            604800                ; Refresh
            86400                ; Retry
            2419200                ; Expire
            604800 )            ; Negative Cache TTL

; name servers – NS und A records
@       IN    NS    ns.blackgate.dmz.
ns      IN    A    192.168.13.2

; 192.168.1.X/24 - A records
router      IN    A    192.168.1.1
wiki        IN    A    192.168.1.10
test        IN    A    192.168.1.17
www     IN    A    192.168.1.23
cloud       IN    A    192.168.1.25
```

Erstellen der Reverse-Zone für das LAN Netzwerk:

```
# vim /var/lib/bind/db.192.168.1
```

```
$TTL    604800
@   IN    SOA     (
            ns.blackgate.dmz.         ; MNAME Record
            admin.blackgate.dmz.         ; Mail von DNS Admin
            2017022001             ; Serial
            604800                 ; Refresh
            86400                 ; Retry
            2419200                 ; Expire
            604800 )              ; Negative Cache TTL

; name servers – NS record
@   IN    NS    ns.blackgate.dmz.

; 192.168.1.X/24 - PTR records
1   IN    PTR    router.blackgate.lan.
10  IN    PTR    wiki.blackgate.lan.
17  IN    PTR    test.blackgate.lan.
23  IN    PTR    www.blackgate.lan.
25  IN    PTR    cloud.blackgate.lan.
```

Erstellen der Forward-Zone für das DMZ Netzwerk:

```
# vim /var/lib/bind/db.blackgate.dmz
```

```
$TTL    604800
@   IN    SOA     (
            ns.blackgate.dmz.         ; MNAME Record
            admin.blackgate.dmz.         ; Mail von DNS Admin
            2017022001             ; Serial
            604800                 ; Refresh
            86400                 ; Retry
            2419200                 ; Expire
            604800 )              ; Negative Cache TTL

; name servers – NS und PTR records
@       IN    NS    ns.blackgate.dmz.
ns      IN    A    192.168.13.2

; 192.168.13.X/24 - PTR records
router          IN    A    192.168.13.1
dns-server  IN    A    192.168.13.2
```

Erstellen der Reverse-Zone für das DMZ Netzwerk:

```
# vim /var/lib/bind/db.192.168.13
```

```
$TTL    604800
@   IN    SOA     (
            ns.blackgate.dmz.         ; MNAME Record
            admin.blackgate.dmz.         ; Mail von DNS Admin
            2017022001            ; Serial
            604800                ; Refresh
            86400                ; Retry
            2419200                ; Expire
            604800 )            ; Negative Cache TTL

; name servers – NS und PTR records
@   IN    NS    ns.blackgate.dmz.
2   IN    PTR    ns.blackgate.dmz.

; 192.168.13.X/24 - PTR records
1   IN    PTR    router.blackgate.dmz.
2   IN    PTR    dns-server.blackgate.dmz.
```

Nach dem erstellen der **Zonen Files**, müssen diese anschliessend noch **korrekt berechtigt** werden!

```
# chown root:bind –R /var/lib/bind && chmod 664 /var/lib/bind/db*
```

Mehr Details zu den Zonen Hier: Aufbau einer Zone

Festlegen der DNS Optionen

Bevor nun jedoch der DNS Server produktiv verwendet werden kann, müssen noch ein paar Optionen in der `named.conf.options` Datei von bind angepasst werden.

```
# vim /etc/bind/named.conf.options
```

```
# Konfigurationsfile /etc/bind/named.conf.options
# Definieren der Optionen unseres Bind-Servers.

options {
        directory "/var/cache/bind";

        recursion yes;                 # Erlaubt rekursive Queries
        allow-transfer { none; };      # Deaktiviert einen Zonentransfer!
        allow-query {
                192.168.0.0/16;        # Erlaubt nur Queries aus dem Netz:
192.168.*
                127.0.0.0/8;
```

```
        };

        forwarders {
                8.8.8.8;                # Findet unser DNS nicht, leitet er
die Anfrage hier weiter
                8.8.4.4;
        };

        auth-nxdomain no;               # conform to RFC1035
#
};
```

Zum Schluss, wird der DNS-Server noch neugestartet, damit unsere neu erstellte Konfiguration übernommen wird und unserer DNS Server ordnungsgemäss funktioniert.

```
# systemctl restart bind9
# systemctl status bind9
```

ISC-DHCP Server

Die nachfolgenden Installationen, werden alle mit dem Benutzer **root** durchgeführt. Deshalb wird als ersten Schritt einmal auf das frisch installierte **Debian / Ubuntu** per **Putty** verbunden und Authentifiziert.

Anschliessend wird das System erstmals auf den neusten Stand gebracht und das Package isc-dhcp-server, welches unseren DHCP-Server enthält installiert:

```
# apt-get update
# apt-get –y upgrade

# apt-get -y install isc-dhcp-server
```

ISC-DHCP Server Konfiguration

Nun geht es um die DHCP Konfiguration. Hierzu editieren wir wieder auf dem Server das Konfigurations-file `/etc/dhcp/dhcpd.conf`.

```
# vim /etc/dhcp/dhcpd.conf
```

```
# DHCP Konfiguration – blackgate.lan
```

```
ddns-update-style none;
default-lease-time 600;
max-lease-time 7200;
authoritative;
log-facility local7;

subnet  192.168.1.0 netmask 255.255.255.0 {

    range 192.168.1.100 192.168.1.180;

    option subnet-mask 255.255.255.0;
    option broadcast-address 192.168.1.255;
    option routers 192.168.1.1;
    option domain-name-servers 192.168.13.2;
    option domain-name "blackgate.lan";

        host wiki-v2 {
               hardware ethernet 00:50:56:00:21:61;
               fixed-address 192.168.1.10;
           option host-name "wiki-v2";
        }
}
```

Nach dem erfolgreichen konfigurieren des DHCP Servers, muss dieser nun noch aktiviert, sprich gestartet werden.

```
# systemctl start isc-dhcp-server
# systemctl enable isc-dhcp-server
```

- https://wiki.ubuntuusers.de/ISC-DHCPD/
- https://help.ubuntu.com/community/isc-dhcp-server

DDNS - Dynamic Domain Name System via RNDC

Alle Computer aus der IP-Range des dynamischen DHCPs, sollen automatisch in die entsprechenden SOA Records eingetragen werden; damit deren Name oder zugewiesenen IP-Adressen vom DNS aufgelöst werden können. Um dieses Vorhaben zu realisieren, wird das ***Dynamic Domain Name System*** DDNS mithilfe von dem Utility **RNDC** realisiert.

Vorarbeit

Im ersten Schritt, wird der von der Installation von bind9 automatisch generierte RNDC-Key in das /etc/dhcp Verzeichnisses unseres DHCP-Servers kopiert! Liegt der DNS und der DHCP-Server nicht auf dem gleichen System, so muss dieser Key, über das Netzwerk mit folgendem Befehl kopiert werden: “`# scp root@IP_DNS_SERVER:/etc/bind/rndc.key /etc/dhcp`”

Anschliessend, müssen beide Keys noch korrekt berechtigt werden!

```
# chown root:bind /etc/bind/rndc.key
# chmod 640 /etc/bind/rndc.key

# chown root:dhcpd /etc/dhcp/rndc.key
# chmod 640 /etc/dhcp/rndc.key
```

ISC-DHCP – Konfigurationsänderungen

Beim DHCP-Server sind die Änderungen schnell durchgeführt! Hier müssen wir lediglich das Hauptkonfigurations-file `/etc/dhcp/dhcpd.conf` in den unten **BLAU** Markierten Sektoren anpassen.

```
# vim /etc/dhcp/dhcpd.conf
```

```
# DHCP Konfiguration – blackgate.lan

# RNDC.key & neue DDNS Optionen
include "/etc/dhcp/rndc.key";

ddns-updates on;
use-host-decl-names on;
update-static-leases on;

ddns-update-style interim;
default-lease-time 600;
max-lease-time 7200;
authoritative;
log-facility local7;

subnet  192.168.1.0 netmask 255.255.255.0 {

        range 192.168.1.100 192.168.1.180;

        option subnet-mask 255.255.255.0;
        option broadcast-address 192.168.1.255;
        option routers 192.168.1.1;
        option domain-name-servers 192.168.13.2;
        option domain-name "blackgate.lan";

        host wiki-v2 {
               hardware ethernet 00:50:56:00:21:61;
               fixed-address 192.168.1.10;
           option host-name "wiki-v2";
        }

        zone blackgate.lan. {
```

```
        primary 192.168.13.2;
        key rndc-key;
        }
        zone 1.168.192.in-addr.arpa. {
        primary 192.168.13.2;
        key rndc-key;
        }

}
```

DNS – Konfigurationsänderungen

Beim DNS-Server werden gleich mehrere Files angepasst. Begonnen wird mit der `named.conf.local` ***Alle Änderungen / Neuerungen sind wieder BLAU markiert.***

```
# vim /etc/bind/named.conf.local
```

```
# Konfigurationsfile /etc/bind/named.conf.local

        include "/etc/bind/rndc.key";

        # INTERN-NETWORK
        zone "blackgate.lan" in {
        type master;
            file "/var/lib/bind/db.blackgate.lan";
            allow-update { key "rndc-key"; };
        };

        zone "1.168.192.in-addr.arpa" in {
            type master;
            file "/var/lib/bind/db.192.168.1";
            allow-update { key "rndc-key"; };
        };

        # DMZ-NETWORK
        zone "blackgate.dmz" in {
            type master;
            file "/var/lib/bind/db.blackgate.dmz";
            allow-update { key "rndc-key"; };
        };

        zone "13.168.192.in-addr.arpa" in {
            type master;
            file "/var/lib/bind/db.192.168.13";
            allow-update { key "rndc-key"; };
        };
```

Als nächstes, damit auch alles wie gewünscht funktioniert, muss nun noch eine Option in der `named.conf.options` Datei angepasst werden.

```
# vim /etc/bind/named.conf.options
```

```
# Konfigurationsfile /etc/bind/named.conf.options

options {
        directory "/var/cache/bind";

        recursion yes;
        allow-transfer { 192.168.0.0/16; 127.0.0.0/8; };
        allow-query { 192.168.0.0/16; 127.0.0.0/8; };

        forwarders { 8.8.8.8; 8.8.4.4; };

        auth-nxdomain no;             # conform to RFC1035
#
};
```

Wichtig: Um nun Fehler zu verhindern, müssen alte DNS Einträge von Geräten, welche nun ihre IP Adresse via ISC-DHCP beziehen sollen; noch aus der Forward Zone entfernt werden.

***Als Beispiel**, wird hier also der gesamte **A-Record** von vmWP1 aus der Zonendatei /var/lib/bind/db.gibbix.lan herausgelöscht.*

Zum Schluss, kann bind9 neugestartet werden.

```
# systemctl restart bind9
```

Fehlerbehebung

Wenn nun schon Server vorhanden waren, die fix in dem DNS eingetragen wurden und diese nun im Log Fehler verursachen; müssen diese folgendermassen entfernt werden:

1. Herunterschreiben der aktuellen Journal-Files in die Zone-Files →> **`rndc sync –clean`**
2. Stoppen des Bind9 Services → **`systemctl stop bind9`**
3. Manuelles bearbeiten der Zonen Files; A-record von Computer oder Server löschen, welcher Probleme macht. (Nur aus Forward-Zone)
4. Speichern und den Bind9 Service wieder Starten!

Last update: **2017/09/29 14:32**