

Konfiguration von Bind

Wir schauen uns nun die Konfiguration von Bind an. Konfigurationen unter Linux sind in der Regel einfache Text-Dateien, welche die nötigen Anweisungen für die Software enthalten.

Grundkonfiguration

Die Konfiguration des BIND-Servers erfolgt über das Verzeichnis **/etc**. Nach der Installation sollten sich hier folgende Dateien finden:

```
named.conf  
named.iscdlv.key  
named.rfc1912.zones  
named.root.key
```

Der Prozess von BIND ist als **named** bekannt. Daher beziehen sich viele der Dateien auf "named" anstelle von "BIND".

Die Datei **named.conf** ist die Haupt-Konfiguration von Bind. Öffnen Sie die Konfiguration nun mit dem Befehl **nano**.

Sie werden nun feststellen, dass die Konfiguration für Bind in gewissen Gruppen zusammengefasst ist, welche durch geschweifte Klammern **{ }** umschlossen werden. In der Gruppe **options** finden Sie die Grundkonfigurationen.

Zeile	Bedeutung
<code>listen-on port 53 { 127.0.0.1; };</code>	Definiert auf welcher IP-Adresse und welchem Port der DNS-Server eingehende Verbindungen annehmen soll. Bei 127.0.0.1 handelt es sich um die localhost Adresse des Servers, der Dienst wird daher nur Verbindungen vom eigenen Server annehmen.
<code>listen-on-v6 port 53 { ::1; };</code>	Dasselbe gibt es auch in einer separaten Variante für IPv6
<code>allow-query { localhost; };</code>	Definiert, wer (welche IP-Adresse) eine DNS-Abfrage stellen darf. Standardmässig ist der Wert auf localhost gesetzt. Der Dienst wird daher nur DNS-Abfragen vom eigenen Server beantworten.
<code>directory</code>	In dem angegeben Verzeichnis werden die Dateien mit den DNS-Informationen (Zonen) abgelegt.
<code>recursion yes;</code>	Definiert ob der Server rekursive DNS-Abfragen bearbeitet oder nicht. Standardmässig ist diese Option auf yes wodurch der Dienst als DNS-Resolver fungiert. Soll der Dienst nur als autoritativer Nameserver arbeiten, dann muss diese Option auf no gesetzt werden.

Die grundlegenden Einstellungen sind soweit in Ordnung. Es muss aber eine Einstellung angepasst werden, damit der DNS-Server Anfragen von unserer IP-Adresse überhaupt annimmt.

Im Kontext von Einstellungen unter Linux spricht man bei den einzelnen Einstellungsmöglichkeiten von Direktiven.

- Die **listen-on** Direktive ist derzeit auf 127.0.0.1 gesetzt. Aus diesem Grund nimmt der DNS-Server keine Verbindungen von extern an. Um das zu ändern, setzen Sie die Direktive auf **any**. Den Port 53 können Sie belassen, da dies der Standard-Port für DNS ist:

```
listen-on port 53 { any; };
```

Damit ist die Basis-Konfiguration abgeschlossen. Im nächsten Schritt werden wir nun eine DNS-Zone einrichten.

Starten des Dienstes

Bis jetzt ist der DNS-Dienst noch nicht gestartet. Mit dem Befehl **systemctl** können wir einen Dienst steuern:

```
systemctl enable named[]Aktiviert den Dienst und trägt diesen im Autostart ein
systemctl disable named[]Deaktiviert den Dienst und entfernt diesen aus dem Autostart
systemctl start named[]Startet den Dienst
systemctl stop named[]Stoppt den Dienst
systemctl restart named[]Startet den Dienst neu
```

Verschaffen Sie sich einen weitergehenden Überblick über systemctl und wie damit ein Dienst verwaltet werden kann auf folgender Seite: <https://www.digitalocean.com/community/tutorials/how-to-use-systemctl-to-manage-systemd-services-and-units-de>

Hilfe Hilfe, der Dienste startet nicht!

Bei fehlerhaften Konfigurationen kann es sein, dass ein Serverdienst nicht starten kann. Hier gibt es verschiedenen Möglichkeiten die Ursache zu finden. Nachfolgend ist eine Meldung ersichtlich, dass der Dienst named (bind) nicht gestartet werden konnte:

```
# systemctl start named.service
Job for named.service failed because the control process exited with error code. See "systemctl status named.service" and "journalctl -xe" for details.
```

Möglichkeit 1: Systemctl gibt Ihnen einen kurzen Auszug der letzten Informationen aus dem Log zurück mit **systemctl status named.service**. Dies sieht wie folgt aus:

```
# systemctl status named.service
● named.service - Berkeley Internet Name Domain (DNS)
   Loaded: loaded (/usr/lib/systemd/system/named.service; enabled; vendor preset: disabled)
   Active: failed (Result: exit-code) since Wed 2022-12-14 15:10:12 UTC; 9s ago
     Process: 4379 ExecStop=/bin/sh -c /usr/sbin/rndc stop > /dev/null 2>&1 || /bin/kill -TERM $MAINPID (code=exited, status=0/SUCCESS)
     Process: 4317 ExecReload=/bin/sh -c /usr/sbin/rndc reload > /dev/null 2>&1 || /bin/kill -HUP $MAINPID (code=exited, status=0/SUCCESS)
     Process: 3093 ExecStart=/usr/sbin/named -u named -c ${NAMEDCONF} $OPTIONS (code=exited, status=0/SUCCESS)
     Process: 4390 ExecStartPre=/bin/bash -c if [ ! "$DISABLE_ZONE_CHECKING" == "yes" ]; then /usr/sbin/named-checkconf -z "$NAMEDCONF"; else echo "Checking of zone files is disabled"; fi (code=exited, status=1/FAILURE)
    Main PID: 3095 (code=exited, status=0/SUCCESS)

Dec 14 15:10:12 ip-172-31-72-77.ec2.internal systemd[1]: Starting Berkeley Internet Name Domain (DNS)...
Dec 14 15:10:12 ip-172-31-72-77.ec2.internal bash[4390]: /etc/named.conf:62: missing ';' before end of file
Dec 14 15:10:12 ip-172-31-72-77.ec2.internal systemd[1]: named.service: control process exited, code=exited status=1
Dec 14 15:10:12 ip-172-31-72-77.ec2.internal systemd[1]: Failed to start Berkeley Internet Name Domain (DNS).
Dec 14 15:10:12 ip-172-31-72-77.ec2.internal systemd[1]: Unit named.service entered failed state.
Dec 14 15:10:12 ip-172-31-72-77.ec2.internal systemd[1]: named.service failed.
```

Es wird ersichtlich, dass in auf der Zeile 62 in der Datei `/etc/named.conf` wohl ein Zeichen fehlt.

Möglichkeit 2: Manchmal möchten Sie auch das gesamte Log einsehen. Bind loggt standardmässig alle Informationen in das Log `/var/log/messages`. Hier können Sie einfach nach dem Stichwort **named** suchen:

```
# grep named /var/log/messages
Dec 14 15:09:15 ip-172-31-72-77 named[3095]: received SIGHUP signal to reload zones
Dec 14 15:09:15 ip-172-31-72-77 named[3095]: loading configuration from '/etc/named.conf'
Dec 14 15:09:15 ip-172-31-72-77 named[3095]: /etc/named.conf:62: missing ';' before end of file
Dec 14 15:09:15 ip-172-31-72-77 named[3095]: reloading configuration failed: failure
```

Auch hier ist die Ursache ersichtlich.

Möglichkeit 3: Bind bietet ein Tool, dass uns erlaubt eine Konfiguration auch zu testen bevor man einen Neustart vornimmt. Mit `named-checkconf` kann während der Laufzeit geprüft werden, ob ein Konfigurationsfehler vorliegt. So kann dieser Fehler behoben werden, **bevor** der Dienst neu gestartet wird. So kann ein Ausfall des Dienstes verhindert werden.

```
# named-checkconf
/etc/named.conf:62: missing ';' before end of file
```

Diese Möglichkeit funktioniert natürlich nur bei Fehlern, welche durch ein Konfigurationsproblem verursacht werden. Wenn andere Fehler vorliegen wie z. B. zu wenig Speicher oder RAM, dann müssen die Informationsn aus dem Log beigezogen werden.

Zugriffsbeschränkung

Tipp: Testen Sie eine DNS-Abfrage wenn der Dienst jeweils gestartet und beendet ist. Notieren Sie die Unterschiede und halten Sie diese für Ihr Testprotokoll wie auch Troubleshooting-Möglichkeiten in Ihrer Dokumentation fest.

Erhalten Sie beim Testen einen REFUSED Fehler? Wenn ja, dann läuft Ihr DNS-Dienst aber es fehlt noch eine Konfiguration.

Was für eine Fehlermeldung haben Sie erhalten? Welche Option wird dafür verantwortlich sein? Prüfen Sie den Abschnitt Grundkonfiguration.

Tipp: Die Erkenntnisse aus der obigen Fragestellung gehört in die Dokumentation zum Testing und Troubleshooting.

Bind erlaubt es, zu steuern, welchen IP-Adressen eine DNS-Abfrage stellen dürfen. Hierzu kann eine Liste mit erlaubten IP-Adressen angelegt werden. Diese sollte am besten im Verzeichnis **/etc/named/** erstellt werden. z. B.

```
# cat /etc/named/zugriff.acl
acl "erlaubte-ips" {
    1. 2. 3. 4;
    2. 3. 4. 5;
    localhost;
    localnets;
};
```

Ihre derzeitige IP-Adresse können Sie unter <https://ip.metanet.ch> herausfinden.

Damit diese Zugriffsliste auch verwendet wird, muss diese nun in der Konfiguration **/etc/named.conf** hinterlegt werden.

Sie können diese ganz unten bei den bestehenden Includes ergänzen:

```
include "/etc/named.rfc1912.zones";
include "/etc/named.root.key";
include "/etc/named/zugriff.acl";
```

Zu guter Letzt, müssen Sie nur noch die Zugriffsliste in der Direktive allow-query angeben:

```
allow-query { erlaubte-ips; };
```

Testen Sie anschliessend erneut und halten Sie Ihre Ergebnisse im Dokument fest.

Revision #6

Created 19 October 2022 21:40:22 by Admin

Updated 15 December 2022 10:54:55 by Admin