

Grundlagen

Als die Verwaltung und Aktualisierung der Namensauflösung über die Host-Datei (/etc/hosts) durch das immer weiter wachsende Internet zu umständlich wurde, mußte eine neue Lösung für die Aufgabe gefunden werden. Lösung dieses Problems war der Domain Name Service (DNS). Der DNS wurde als dezentralisiertes, hierarchisches System entworfen. Die bekannteste DNS-Implementierung auf UNIX/Linux-Plattformen ist das Programmpaket BIND vom ISC.

BIND besteht aus zwei Teilen, die unabhängig voneinander betrieben werden können: die Client-Seite wird Resolver genannt und generiert die DNS-Abfragen (Queries), die Server-Seite übernimmt das Programm named und beantwortet eingehende Anfragen.

Resolver

Der Resolver erhält eine Anfrage nach einem DNS-Eintrag, generiert die DNS-Abfrage und sendet sie zu den eingestellten DNS-Servern. Der DNS-Server verarbeitet die Anfrage und sendet die Antwort dem Resolver zurück, der wiederum leitet die Antwort an das aufrufende Programm weiter. Für das manuelle Abfragen von DNS-Einträgen kann das Programm nslookup verwendet werden, viele Programme verwenden aber die Resolver-Bibliotheken direkt um DNS-Queries zu erzeugen. Die Konfiguration erfolgt über die Datei /etc/resolv.conf, in der die DNS-Server, die Suchlisten (Domainnamen, die an Hostnamen angefügt werden können) und eine Sortierungsliste eingetragen werden können.

DNS-Server

Der DNS-Server verwaltet die Domänen und IP-Adressen in sogenannten Zonen. Eine Sammlung von Domain-Informationen, die in einer Domain-Datenbankdatei enthalten ist, wird als Zone bezeichnet.

Eine Umsetzung von Domain-Namen in IP-Adressen wird allgemein als Lookup bezeichnet, die Umsetzung IP-Adresse nach Domain-Name als reverse Lookup. Für den Lookup oder den reverse Lookup bestehen mehrere Möglichkeiten, wie der DNS-Server Anfragen beantworten kann:

1. der DNS-Server hält selber die Information über das angeforderte Objekt in seiner Domain-Datenbankdatei und ist autoritativ für diese Zone zuständig;
2. der DNS-Server hat die Datenbankdatei der entsprechenden Zone von einem anderen DNS-Server heruntergeladen und ist für diese Zone als Backup-DNS konfiguriert; kann die Anfrage anhand der heruntergeladenen Zone selber beantworten;
3. für die entsprechende Zone ist ein anderer DNS-Server fest eingetragen, der befragt werden soll (Forwarding-Zone)
4. für die Zone ist kein spezifischer Eintrag im DNS durchgeführt, so daß
 - (a) bei eingestelltem Forward-Only nur der eingestellte Forward-DNS-Server befragt wird;
 - (b) die DNS-Hierarchie durchlaufen wird, um den DNS-Server zu finden, der für das Objekt zuständig ist (angefangen bei den Root-Servern);

Erhaltende Antworten von anderen DNS-Servern werden zwischengespeichert, um bei einer erneuten Anfrage nach dem Objekt eine Antwort aus dem lokal vorhandenen Cache zu generieren. Die Antwort wird solange im Cache gehalten, bis seine Lebenszeit (TTL) abgelaufen ist oder der DNS-Dienst neu gestartet wird (DNS-Cache befindet sich im Arbeitsspeicher).

Konfiguration

Für BIND ist standardmäßig die Konfigurationsdatei /etc/named.conf zuständig. In dieser Datei werden neben globalen Optionen die einzelnen Zonen mit ihrem Typ definiert (master, slave, forward, hint). Die einzelnen Zonen-Dateien sind häufig in /var/named zu finden.

Eigenschaften BIND8

- kann sowohl master-, slave, forward- und hint-Zonen verwalten;
- ACL-Kontrolle generell auf BIND als auch auf einzelne Zonen;
- Dynamische DNS-Aktualisierung möglich;
- Ausgeprägte Loggingfunktionen, einzeln einstellbar für jede Zone und Global;
- Bindung an spezifisches Interface;
- Unterstützt neue SRV-Einträge in Zonen;