

| Logging

Abschliessend richten Sie noch die Log-Funktion für den Dienst ein. Das Log enthält alle relevanten Informationen aus dem Betrieb des Dienstes und erlaubt im Nachhinein Fehler nachzuvollziehen.

Passen Sie als erstes den Abschnitt **logging** in der Datei **/etc/named.conf** wie folgt an:

```
logging {  
    channel default_file {  
        file "/var/log/named/default.log" versions 3 size 5m;  
        severity dynamic;  
        print-time yes;  
    };  
  
    channel resolver_file {  
        file "/var/log/named/resolver.log" versions 3 size 5m;  
        severity debug 11;  
        print-time yes;  
    };  
  
    channel queries_file {  
        file "/var/log/named/queries.log" versions 3 size 5m;  
        severity debug 11;  
        print-time yes;  
    };  
  
    channel database_file {  
        file "/var/log/named/database.log" versions 3 size 5m;  
        severity debug 11;  
        print-time yes;  
    };  
  
    category default { default_file; };  
    category queries { queries_file; };  
    category database { database_file; };  
    category resolver { resolver_file; };  
  
};
```

Nun müssen die dazugehörigen Log-Dateien erstellt und mit den richtigen Berechtigungen versehen werden:

```
mkdir -p /var/log/named/  
  
touch /var/log/named/default.log  
touch /var/log/named/resolver.log  
touch /var/log/named/queries.log  
touch /var/log/named/database.log  
  
chown named: /var/log/named/default.log  
chown named: /var/log/named/resolver.log  
chown named: /var/log/named/queries.log  
chown named: /var/log/named/database.log
```

Anschliessend können Sie den Dienst neu starten und in das Verzeichnis **/var/log/named** wechseln.

Sie haben nun verschiedene Möglichkeiten, die Informationen in den Logs auszuwerten:

tail -f: Mit dem Befehl "tail -f" können Sie die Log-Informationen fortlaufend ausgeben. Mit der Tastenkombination CTRL + C können Sie die Ausgabe wieder schliessen.

```
tail -f /var/log/named/resolver.log
```

Wenn Sie nur nach den Informationen einer bestimmten Domain suchen, macht es Sinn wenn Sie die Ausgabe mit **grep** filtern:

```
tail -f /var/log/named/resolver.log | grep domain.ch
```

Mit dem * als Wildcard-Zeichen, können Sie auch gleichzeitig mehrere Logdateien ausgeben:

```
tail -f /var/log/named/*.log
```

grep: Mit grep können Sie auch direkt innerhalb der Dateien suchen. Damit durchsuchen Sie dann den gesamten Inhalt der betreffenden Logdatei:

```
grep domain.ch /var/log/named/resolver.log
```

Mit dem * als Wildcard-Zeichen, können Sie auch gleichzeitig mehrere Logdateien durchsuchen:

```
grep domain.ch /var/log/named/*.log
```

Bedeutung Log

- Default: Im Default-Log werden die normalen BIND-Informationen geloggt.
- Queries: Hier werden die eingehenden DNS-Anfragen verzeichnet.
- Database: Hier werden abfragen in die lokale DNS-Datenbank (Cache) verzeichnet.
- Resolver: Hier werden die DNS-Abfragen verzeichnet, welcher der Resolver auf andere DNS-Server macht.

Dokumentation

Notieren Sie in der Dokumentation welche Logs sich wo befinden und was diese bedeuten. Machen Sie ggf. auch ein zwei Beispiele und beschreiben Sie, was im Log aufgezeichnet wird.

Revision #4

Created 15 December 2022 00:27:52 by Admin

Updated 15 December 2022 11:00:51 by Admin