

DNS Zonen erstellen

Diese Anleitung beschreibt, wie Sie eine generische DNS-Zone erstellen können. Sie benötigen ggf. mehrere DNS-Zonen um die Anforderungen Ihres Auftrags zu erfüllen. Legen Sie als erstes die nachfolgende Test-Zone an und anschliessend die benötigten DNS-Zonen.

DNS-Zonen

Eine DNS-Zone benötigt zwei Teile:

- Einen Eintrag in der Datei `/etc/named.conf`, welcher dem DNS-Server mitteilt das eine Zone existiert und was für ein Typ die Zone ist.
- Der eigentliche Inhalt der Zone, welcher als eigene Datei abgelegt ist.

Named.conf

Fügen Sie nun ganz am Ende der Datei `/etc/named.conf` folgenden Abschnitt ein:

```
zone "test.tbz" {  
    type master;  
    file "/var/named/test.tbz";  
};
```

- Sie teilen damit dem DNS-Server mit, dass nun die Konfiguration für die DNS-Zone **test.tbz** folgt.
- Dabei setzen Sie den Typ der DNS-Zone mit der Direktive **type** auf **master**.

- Mit der Direktive **file** geben Sie den Pfad zur Datei mit dem Inhalt der DNS Zone an. Diese Datei existiert derzeit noch nicht und muss im nächsten Schritt von uns angelegt werden.

Bei vielen Zonen wird die Datei `named.conf` schnell mal unübersichtlich gross. Aus diesem Grund empfiehlt es sich hier analog der Zugriffsliste eine separate Datei mit den DNS-Zonen unter `/etc/named/` (z. B. `/etc/named/dns.zones`) zu erstellen und diese mit `include` einzubinden. **Setzen Sie diese Lösung für Ihre benötigten DNS-Zonen um.**

Das Zonen-File

Wechseln Sie nun in das Verzeichnis `/var/named` und erstellen Sie eine neue Datei mit dem Namen **test.tbz**

In dieser Datei fügen Sie nun den nachfolgenden Inhalt ein:

```
$TTL      600
@         IN      SOA      ns1.test.tbz. admin.test.tbz. (
                        2      ; Serial
                        604800 ; Refresh
                        86400  ; Retry
                        2419200 ; Expire
                        604800 ) ; Negative Cache TTL
;
@         IN      NS       ns1.test.tbz.
@         IN      A        8.8.8.8
ns1       IN      AAAA     <IP des DNS-Servers>
```

Sehen wir uns das Zonen-File etwas genauer an:

- Die TTL (Time to life) definiert, wie lange ein DNS-Resolver die Zonen-Informationen im Cache behalten wird. Eine niedrige TTL wird die Last auf dem Server erhöhen, da ein DNS-Resolver zur Abfrage der selben DNS-Zone mehr Requests stellen wird. Der Wert wird in Sekunden angegeben.
- Der Origin definiert den Namen der DNS-Zone.
- Es folgt ein Block mit den Basis Zonen-Informationen, hier ist vor allem die **Serial** relevant. Bei der Serial handelt es sich sozusagen um eine Version der Zone, bei jeder Anpassung muss

die Serial erhöht werden, damit Slave-DNS-Server eine Änderung in der Zone erkennen können.

DNS-Zone überprüfen.

Ist der Inhalt einer DNS-Zone nicht korrekt, kann der DNS-Dienst nicht mehr gestartet werden. Aus diesem Grund sollte die Zone vor einem Neustart überprüft werden.

```
named-checkzone test.tbz /var/named/test.tbz
```

DNS-Zone testen

Verwenden Sie die bekannten Tools um zu testen, ob die von Ihnen angelegten DNS-Zonen funktionieren. Im einen weiterführenden Test, können Sie Ihren Nameserver auch bei Ihrem Windows hinterlegen und die betreffenden Domains aufrufen.

Revision #9

Created 20 October 2022 08:17:35 by Admin

Updated 22 December 2022 10:33:40 by Admin