Nasıl DNS Hizmeti Verebilirim?

Linux Life'ın bu ilk sayısından hepinize merhaba. Bu köşede her ay yeni bir konuyu derinlemesine ele alacak ve konu ile ilgili tüm temel "Nasıl Yaparım?" sorularına yanıt arayacağız. Konu önerilerinizi e-posta ile bizlerle paylaşmaktan çekinmeyiniz. Bu ilk sayımızda bir Linux sistemi ile nasıl birden fazla alan adı için DNS sunucu hizmeti sağlayanabileceğini göreceğiz. Bu yazıyı okuduktan sonra kendi DNS sunucunuzu kurabilecek ve dilediğiniz kadar alan adı için DNS sunucu hizmeti sağlayabileceksiniz.

DNS (*Alan Adı Sistemi*), bilgisayar isimleri ile IP adresleri arasında her iki yönde dönüşüm sağlayan sistemdir. Bu sistem mevcut olmasaydı, tüm web sitelerinin IP adreslerini ezberlemek zorunda kalırdık. İnternet'in tanımlanan ilk protokolleri arasında bulunan DNS protokolü bu zorunluluğu ortadan kaldırmaktadır.

DNS sisteminin önemli bir özelliği, DNS sunucularında meydana gelebilecek arızaları ele alabilmesidir. Her alan adı kaydı ile birlikte tanımlanan bir ana (ing. primary) ve çok sayıdaki ikincil (ing. secondary) DNS sunucuları, bir sunucunun çalışmaz hale gelmesi durumunda bile diğerlerinin devam etmesi sayesinde hizmetin aksamamasını sağlar.

DNS hizmeti sunmak üzere en yaygın biçimde kullanılan yazılım İnternet Yazılım Konsorsiyumu tarafından üretilen ve desteklenen Bind'dır. Bu yazının yazıldığı tarihteki güncel sürümü 9.1.3'tür. Bind, hemen hemen tüm Linux dağıtımları içerisinde yer alan önemli bir yazılımdır. Eğer dağıtımınız içerisinde yer alan Bind'ın sürümü ftp://ftp.isc.org/isc/bind9 dizini altında yer alan güncel sürümden eski ise yeni sürümü çekmenizi ve kurmanızı öneririz.

Kurulum

Bind'ın güncel sürümü dağıtımınızın sağlayıcısı tarafından düzenli olarak bir "paket" halinde size sağlanacaktır. Kullandığınız dağıtımın (Red Hat, Debian vb.) sağlayıcısı Bind'ın güncel sürümünü size sunamıyorsa kaynak kodlarını çekip derleyerek kurabilirsiniz.

Kaynak kodu çekmeniz durumunda aşağıdaki beş komut ile kurulumu gerçekleştirebilirsiniz:

Yapmanız gerekenler (i) güncel paketi çekmek, (ii) paketi sisteminiz üzerinde uygun bir dizin altına açmak, (iii) yazılımın yapılandırılmasını sisteminize uygun bir biçimde gerçekleştirmek, (iv) yazılımı derlemek ve (v) kurulumu sağlamak biçiminde özetlenebilecek ve her biri bir komuta karşılık gelen beş adımdır:

```
$ tar xvzf bind-9.1.3.tar.gz
```
Kaynak kod arşivini sisteminiz üzerinde açın

```
$ cd bind-9.1.3
```
Kaynak kodların bulunduğu dizine geçin

```
$ ./configure
```
Derleme öncesi ayarlarının sisteminize göre yapılmasını sağlayın

```
$ make
```
Kaynak kodların derlenmesini ve bağlanmasını sağlayın

```
$ make install
```
Derlenmiş programların ve belgelerin kurulmasını sağlayın

Bu komutları verdiğinizde Bind, /usr/local dizini altına kurulmuş ve çalışmaya hazır durumda olacaktır. Bu adımdan sonra yapılması gereken hangi alanlar için DNS hizmeti verilecek ise, bu alanlar için gerekli ayarların ve tanımların yapılması olacaktır.

Alan Dosyaları

Hizmet verilecek her alan ile ilgili tanımlar alan dosyası (ing. *zone file*) adı verilen dosyalar aracılığı ile gerçekleştirilir. Birden fazla alan adı için DNS hizmeti sağlanacak ise her bir alan için ayrı alan dosyaları tamamlanmalıdır. Alan dosyalarının tümünü aynı dizin altına kaydedilmesi gerekmektedir. Örnek bir alan dosyası içeriği aşağıda verilmektedir.

```
$ORIGIN dayioglu.net
$TTL 1D
@      IN SOA      trinity.dayioglu.net.     burak.dayioglu.net. (
                                        5; Seri Numarasi
                                        10800; Uc saatten sonra guncelle
                                        3600; Bir saatten sonra tekrar dene
                                        604800; Bir hafta sonra gecersiz kilinsin
                                        10800; Minimal yasam suresi – TTL
                                        )
; DNS Sunuculari
dayioglu.net.                   IN NS  trinity.dayioglu.net.
dayioglu.net.                   IN NS   probe.dayioglu.net.
; E-posta Sunuculari
dayioglu.net.                   IN MX 0 mail1.dayioglu.net.
dayioglu.net.                   IN MX 10 mail2.dayioglu.net.
; Doğrudan istemler için
dayioglu.net                    IN A   10.1.2.3
; dayioglu.net'in tum bilgisayarlari
trinity                         IN A   10.1.2.3
probe.dayioglu.net.             IN A  10.1.2.4
; tum takma ad tanimlari
www                             IN CNAME     trinity
mail1                           IN CNAME     trinity
mail2                           IN CNAME     probe
```

Alan dosyaları ana DNS sunucusu üzerinde tanımlanır ve tanımlanan ikincil sunucular tarafından periyodik olarak kopyalanarak kullanılır.

İlk satırda başlayan ve dokuzuncu satırdaki parantez kapama simgesi ile biten bölüm alan adını ve yetki kaynağını (ing. *Source of Authority* – SOA) tanımlamak için kullanılır. Yukarıdaki örnek alan dosyası, `dayioglu.net` alan adı için düzenlenmiştir; ilk satırda kullanılması zorunlu olmamakla birlikte $ORIGIN tanımı ile bu dosyanın dayioglu.net için olduğu bildirilir. Üçüncü satırın hemen başında yer alan "@" işareti dosyanın tümü boyunca alan adına karşılık gelecektir.

DNS sisteminde sorguların (ve yanıtların) sıklığını azaltmak için ön-bellekleme (ing. *caching*) tekniği kullanılmaktadır. Bir sorgulama yapıp yanıtını alan istemciler, bu sorguyu DNS sunucuya sunucu tarafından

belirlenen bir süre boyunca sormaz, daha önce aldıkları yanıtı geçerli kabul ederek işlem yaparlar. Bu süre en az yaşam süresi (ing. *minimum TTL*) olarak adlandırılır. Ön-bellekleme düzeneği sunucuların yükünü ve ağ trafiğini ciddi biçimde azaltmaktadır. Kurulma aşamasında, sıkça adres değişikliklerinin yapıldığı bir ağ üzerinde ön-bellekleme süresi alabildiğine kısa seçilirken oturmuş ve artık nadiren değişikliklerin yapıldığı bir ağda ön-bellekleme süresi mümkün olduğunca uzun seçilmelidir. Her alan adı için ön-tanımlı bir en az yaşam süresi ana DNS sunucusu tarafından belirlenir; yukarıdaki örnekte $TTL yanında yer alan 1D, bir günlük bir süreye işaret etmektedir. Sorgulama yapıp yanıt alan istemciler bir gün süre ile yanıtı koruyacak, aynı sorgulamayı tekrar yapmayacaktır.

Yaşam süresinin yanında yer alan IN anahtar kelimesi bu alanın bir İnternet alanı olduğunu SOA ise yetki kaynağı tanımının başlamakta olduğunu belirtir. SOA'nın ardından gelen `trinity.dayioglu.net.` ile bu alan adının ana DNS sunucusunun `trinity` isimli bilgisayar sistemi olduğu ifade edilmektedir. Alan adının ve DNS sunucularının sonunda yer alan "." işareti unutulmamalıdır; "." işaretinin kullanımı son derece önemlidir.

Yetkili DNS sunucu tanımından hemen sonra alan adı için sorumlu kişinin e-posta adresi verilmektedir. "@" işareti yerine "." işareti bilinçli olarak kullanılmıştır. Alan adı yetkilisi olarak burak@dayioglu.net işaret edilmektedir. Bireysel alan adları için bireysel sorumlu adresleri kabul edilebilir ise de, kurumlar söz konusu olduğunda tanımlanan adreslerin kişilerden bağımsız seçilmesi özellikle önerilmektedir. Böylece, tanımlanan sorumlunun kurumdan ayrılması durumunda e-posta adresinin geçersiz kılınması tehlikesi önlenebilir. Sorumlu e-posta adresi olarak ilgili birden fazla kişiye dağıtım sağlayacak bir grup adresinin kullanılması önerilmektedir. Bu adres, İnternet kullanıcısı herkes tarafından sorgulanabilecek ve teknik problemler olması durumunda iletişim için kullanılacaktır.

Parantez işaretleri arasında yer alan beş satırlık bölüm zaman ayarları ve ikincil DNS sunucuları ile senkronizasyon ile ilgilidir. Bir alan adına ilişkin her türlü kayıt değişikliği işlemi yalnızca ana DNS sunucu üzerinde yapılır.

İkincil DNS sunucuları periyodik olarak ana DNS sunucu ile iletişime geçerek güncellemenin var olup olmadığını sorgular ve var ise güncel kayıtları toplu halde alır ve bu yeni bilgilerin ışığında hizmet vermeye başlarlar. Bu güncel bilgi olup olmadığı sorgusu ilk sayı olan "`seri numarası`" aracılığı ile yapılmaktadır. Alan adınıza yeni bir kayıt eklediğinizde bu sayıyı bir önceki değerinden daha büyük bir sayı oalcak şekilde ayarlamanız gerekmektedir.

Parantezler içinde bulunan ikinci sayı olan "`güncelleme zamanı`" ikincil DNS sunucularının birincil sunucuya ne kadar zaman aralıkları ile güncel bilgi sorgulması yapılacağını belirtir. Eğer yerel ağınız daha oturmamış ve sıkca değişen bir yapıya sahip ise bu sayıyı düşük tutmanız önerilir. Bu zamanı küçük tutmanızın yerel ağınıza bir trafik yükü getireceğini unutmayınız.

Üçüncü sayı olan "`tekrar deneme zamanı`" ise ikinci sayı ile belirtilen güncelleme işlemi başarısız olduğunda bu işlemi ne kadar süre sonunda tekrar denemesi gerektiğini belirtmektedir.

Dördüncü sayı olan "`geçersizlik zamanı`" ise ikincil sunucuların birincil sunucuya belirtilen süre içerisinde güncelleme amacı ile ulaşamaz ise kayıtların geçersiz hale gelmesi ve gelen istemlere cevap verilmeme süresidir.

Son sayı olan "`minimal yaşam süresi`" (ing. Time-To-Live,TTL), herhangi bir sorgu ile üçüncü sunucular tarafından öğrenilen bir bilgisayarımızın IP'sinin üçücü sunucuda ne kadar süre ile geçerli kalacağını belirtir. Bu durumu basit bir örnek ile açıklayalım.

TTL'iniz 3 saat olarak ayarlanmış olsun ve sisteminizde www.dayioglu.net kaydı olsun. Sisteminiz dışarısından her hangi bir yerden internet'e bağlanan kişi t zamanında `www.dayioglu.net` adresine bağlanmış olsun. Sizde t+1 zamanında `www.dayioglu.net`'in IP'sini değiştirdiğinizi varsayalım. Sonuçta t zamanında size bağlanmış olan kişi t'den 3 saat geçene kadar sizin yapmış olduğunuz değişikliği fark edemeyecektir.

İkincil Sunucular ile ilgili ayarlar yapıldıktan sonra alan adımızın esas ayarlarının yapıldığı bölüm yer almaktadır. Bu kısımda alanımızın DNS sunucuları, posta alış-verişçileri (ing. Mail Exchanger, MX), alanın makinaları ve alan makinalarını işaret eden takma adları olacaktır.

İlk önce ayarlanması gereken alan adımızın DNS sunucularıdır. Alanımızın DNS sunucularını ayarlamak için satır başına alan adımızı yazdıktan ve sonuna nokta koyduktan sonra (örneğimizde dayioglu.net.) "`IN NS`" (kısaltma: in Name Server) yazıyor ve peşine DNS sunucularımızı her biri ayrı bir satırda olacak şekilde yazıyoruz. Burada kullanılması önerilen eğer alan adı sunucunuz alanınız ile aynı alan içerisinde olacaksa, dosyanın ilerleyen kısımlarında belirtilmiş olan kayıtlardan birini kullanmaktır. Tanımlanan sunucuların hangisinin birincil hangilerinin ikincil sunucular olduğu bu ayar dosyası aracılığı ile değil, bind'in ana ayar dosyası aracılığı ile yapılmaktadır.

Bundan sonra ayarlanması gereken kısım ise posta alış-verişçilerini ayarlamaktır. Bu alan ile e-posta kullanılmak isteniyorsa ayarlanması zorunlu bir alandır. Bu tanım DNS sunucuları tanımına benzemesine rağmen "`IN MX`" den sonra posta sunucusunun önceliğinin verilmesi gerekmesidir. Posta sunucusunun önceliği posta sunucuları arasında tercih belirlemek için kullanılır. Bahsi geçen alan adı için öncelikle önceliği düşük olan posta sunucuna posta göndermeye çalışır. Eğer bu sunucuya ulaşılamaz ise önceliği daha fazla olan sunucuya posta gönderilir.

Bir sonraki aşama ise alan adının kendisi için bir IP atanmasıdır. Eğer alan adınızın yanlızca adı ile ulaşılmasını (başında www olmadan vb) istediğinizde ayarlamanız gerekmektedir. Bu adım için "`IN A`" (kısaltma: in Address) tanımlamanız gerekmektedir. Tanımlama işlemi DNS sunucu tanımlaması ile aynıdır. Tek farkı "`IN A`" tanımından sonra IP adresi vermeniz gerekmesidir.

Bu temel ayarları yaptıktan sonra esas tanımlamaların yapılacağı bölüm gelir. Bu bölümde alanımıza dahil olan IP'ler ile bilgisayar isimlerini eşleştiririz. Bu eşleştirme işlemi için önce bilgisayar adımızı alan adı ile birlikte yada alan adına gerek kalmadan yazarız. Dikkat edilmesi gereken nokta bilgisayar adı yazıldıktan sonra "." karakterinin önemidir. Makina adını yazdıktan sonra "." karakteri konumaz ise sunucumuz alan adını otomatik olarak bilgisayar adına ekleyecektir. Eğer bilgisayar adlarını tam olarak yazar iseniz sonuna nokta koymalısınız.

Nasıl DNS Hizmeti Verebilirim?

Esas tanımlamalar bittikten sonra "takma adlar" kesimi başlar. Takma adlar kesimi de esas tanımlamalar ile aynı biçimde yapılır. Takma adları belirtmek için "IN CNAME" (kısaltma: in CanonicalName) kullanılır. "IN CNAME" in sağ tarafında ise bir IP bulunamaz. Burada bir bilgisayar adının yer alması zorunludur. Örneğimizde `mail1.dayioglu.net` makinası aslında `trinity.dayioglu.net`'i göstermektedir. Yani `trinity.dayioglu.net`'in IP'sini değiştirdiğimizde `mail1.dayioglu.net`'in göstermekte olduğu IP'de değişecektir.

Ayar dosyamızda eğer bir not almak ister isek satır başında ";" karakteri kullanarak bahsi geçen satırı yorum satırı haline getirebiliriz.

DNS Kayıt Çeşitleri

Yazımızın başında DNS'in bilgisayar isimlerinden IP'lere geçiş için bir protokol olduğunu söylemiştik. Benzer şekilde DNS IP'lerden bilgisayar isimlerine geçişleride sağlamaktadır. Bilgisayar isimlerinden IP'lere geçiş "Doğrudan Alanlar" (ing. forward zones) aracılığı ile yapılırken IP'lerden bilgisayar isimlerine geçiş "Tersten Alanlar" (ing. reverse zones) aracılığı ile yapılır.Tersten alanların kaydı da aynı doğrudan alanlar gibi yapılmakta olup farkı tersten kayıtlarda takma adlar ve posta alış-verişçileri için kayıt olmamasıdır. Bir IP'nin ait olduğu alan IP'nin ilk üç rakamının tersten yazılmasından sonra sonuna `IN-ADDR.ARPA` eklenmesi ile oluşur. Yine örneğimizden yola çıkarak 10.1.2.4 IP'sini barındıran alanın alan dosyası aşağıdaki gibi olacaktır.

```
$ORIGIN 2.1.10.IN-ADDR.ARPA
$TTL 1D
@      IN SOA      trinity.dayioglu.net.     burak.dayioglu.net. (
                                        5; Seri Numarasi
                                        10800; Uc saatten sonra guncelle
                                        3600; Bir saatten sonra tekrar dene
                                        604800; Bir hafta sonra gecersiz kilinsin
                                        10800; Minimal yasam suresi – TTL
                                        )
; DNS Sunuculari
2.1.10.IN-ADDR.ARPA.            IN NS  trinity.dayioglu.net.
2.1.10.IN-ADDR.ARPA.            IN NS  probe.dayioglu.net.
; Alan adı kayıtları
3                   IN PTR       trinity.dayioglu.net.
4                   IN PTR       probe.dayioglu.net.
```

Bu dosyada dikkat edilmesi gereken "IN PTR" (kısaltma: in PoinTeR) kaydından sonra yer alan bilgisayar isminin tam adı ile yazıldıktan sonra "." karakteri ile sonlandırılması gerektiğidir. Dosyanın başında bulunan alan ise aynı "`doğrudan alanlar`" gibi ayarlanmaktadır.

Nasıl DNS Hizmeti Verebilirim?

Ana Ayar Dosyası

Bind'in ana ayar dosyası `/etc` yada `/usr/local/etc` dizini altında bulunan `named.conf` dosyasıdır. Bu dosya basit olarak bind ile ilgili genel ayarları, sunucunun hizmet vereceği alanları belirler. Temel bir dosya aşağıdaki gibidir.

```
options {
       directory "/etc/domain";
}

zone "." {
       type hint;
       file "named.ca";
};
zone "dayioglu.net" {

       type master;
       file "dayioglu.net.forward";
}
zone "2.1.10.IN-ADDR.ARPA" {
       type master;
       file "dayioglu.net.reverse";
};
zone "zerrin.net" {

       type master;
       file "zerrin.net.forward";
}
zone "carnage.net" {

       type slave;
       file "carnage.net.slave";
       masters {n1.carnage.net;};
}
```

Bind'in ayar dosyasının ilk satırı ile başlayan "`seçenekler`" (options) kısmı bind'in gelen ayarları, işlemesi ve logları ile ilgili ayarların verildiği kısımdır. Örneğimizdeki seçenekler içinde yer alan directory komutu sunucunun alan adı ayar dosyalarını nereye koyduğunu belirtmektedir.

İlk alanımız olan "`zone "."`" (alan kök) ise bind'in bir alan adı sorgusuna kendisi cevap veremediği durumda hangi alan adı sunucularına danışacağı bilgisini içerir. "." özel bir alan olup "`kök sunucular`" (ing. root-cache) olarak adladırılan 9 sunucuyu belirtir. Bu "." Alanı ile ilgili kayıtlar ayar dosyanızda yer almaz ise bir bilgisayar ismi sorgunuzda bilgisayar sizin alanınızda değil ise cevap alamazsınız.

İkinci alanımız olan "`zone "dayioglu.net"`" `dayioglu.net` alan adı için gerekli ayarları içermektedir. Bu alanın içinde tanımlı olan "`type master;`" bu alan adı için ayarlamış olduğumuz sunucunun ana DNS sunucusu olduğunu göstermektedir. "`file "dayioglu.net.forward"`" ise daha önce açıklayarak

oluşturmuş olduğumuz alan adı dosyasının (ing. zone file) dosya sistemindeki adıdır. Örneğimizde `dayioglu.net` için ayar dosyasının "`/etc/domain/dayigoulu.net.forward`" yolunda olması beklenmektedir.

Tersten alan adlarıda aynı doğrudan alan adları gibi tanımlanır ve ayarları yapılır. Ana ayar dosyasında yapılması gereken ilaveten başka bir işlem yoktur. Alan kısmına ("`zone`") yukarıda açıklamış olduğumuz biçimde `IN-ADDR.ARPA`'lı metni yazmanız yeterli olacaktır.

Tabi ki bir DNS sunucusu birden çok alan için hizmet verebilir. Bu durumda yapmamız gereken yeni bir alan ("`zone`") eklemekten ibarettir. Örneğimizde sunucumuza "`zerrin.net`" alanınında ana sunucusu olması gerektiğini ayarladık.

İkincil DNS sunucu ayarında ise aynı birincil sunucu ayarında olduğu gibi önce alan adımız için bir alan bölümü açıyoruz. Sonra tür kısmna ("`type`") kısmında "`slave`" yani ikincil sunucu diyoruz. Alan dosyası kısmını ("`file`") ise önceden varolmayan bir dosya olarak veriyoruz. Unutmayınız slave alanlar için dosya yaratmanıza ve ayarlamanıza gerek yoktur. İkincil DNS sunucular bahsi geçen dosyayı noktalı virgüller ile ayrılmış olan ana sunucular ("`masters`") kısmında belirtilen ana DNS sunucusundan alarak otomatik olarak oluşturacaklardır.

Ayarların Güncellenmesi

Bir ayar dosyasına kayıt eklediğimiz de yada yeni bir alan adına hizmet vermek üzere ayarlamalarınızı yaptığınızda yapmış olduğunuz değişiklikler aynı anda işleme girmez. Yaptığınız değişikliklerin geçerli olabilmesi için sunucunun tazeleme yapması gerekmektedir. Bu amaç ile eğer dağıtımınızla birlikte gelmiş olan bir bind kullanıyorsanız yapmanız gereken yanlızca "`/etc/rc.d/init.d/named reload`" demek olacaktır. Eğer kendi sunucunuzu derlemiş iseniz yapmanız gereken çalışmakta olan "`named`" programının görev numarasını öğrenip ("`ps ax|grep named`") en düşük görev numarasına sahip `named` görevini öğrenmek ve bu göreve `-HUP` sinyali göndermek ("`kill -HUP görevnumarası`")olacaktır.

Sonuç

Bu belge ile siz okurlarımıza bir DNS sunucusunun kurulumunu ve tanımlamalarının yapılamasını anlatmaya çalıştık. Ayar dosyalarında oynamalarda bulunarak daha fazla sayıda alana DNS hizmeti sunmanızda hiçbir sakınca yoktur. Temel olan DNS ayarları bunlardan ibaretdir. Umarız ki bu belge sizin için yararlı olmuştur.

Kerem ERZURUMLU – kerem@linux.org.tr

Burak DAYIOĞLU – burak@metu.edu.tr