



نصب و راه اندازی سرویس (DNS (Domain Name Service)

گردآورنده: علی محمد حسینی

معرفی DNS

در این فصل قصد داریم با یکی از سرویسهای مهم اینترنت که در اکثر ISPها استفاده می شود آشنا شویم. تمام ارتباطات اینترنتی از طریق آدرس IP صورت می گیرد و از آنجا که به خاطر سپردن آدرسهای IP تمام دستگاهها ممکن نیست، لذا نیاز به سیستمی است که وظیفه آن نگهداری نام و آدرس IP سرورها در شبکه و پاسخ به تقاضاهای رسیده برای بدست آوردن آدرس IP سرویس دهنده ها می باشد.

لذا سرور DNS، آدرس IP معادل اسامی داده شده را که این اطلاعات در یک بانک قابل دسترسی برای عموم قرار دارند، بر می گرداند.

DNS serverها به سه دسته تقسیم می شوند:

* Master یا Primary

* Slave یا secondary

* Caching

مفاهیم مهم DNS

قبل از تشریح نحوه نصب یک سرور DNSها ابتدا مفاهیمی را در زیر بیان می نمایم.

* DNS client و DNS serverها مجزا می باشند: هر کامپیوتر لینوکس که امکانات شبکه ای داشته باشد نرم

افزار DNS-client را دارد که معمولا آن را Resolver می نامند. این برنامه برای یافتن آدرس IP مربوط به

یک نام، به ترتیب DNS serverهایی را که نامشان در فایل `/etc/resolv.conf` نوشته شده است، جستجو



Ahoo Engineering Group

می‌کند. نرم افزار DNSserver متکی به فایل `/etc/named.conf` و فایل‌های مرتبط با نواحی تعریف شده در داخل آن، می‌باشد.

* `zone`: برای تعریف مشخصات `host`های موجود در `Domain`، از مجموعه‌ای از اطلاعات استفاده می‌کنیم که اصطلاحاً `zone` نامیده می‌شود. یعنی برای تعریف `host`های شبکه و یا تعریف یک `subdomain` جدید باید یک `zone` یا نام `Domain` یا `subdomain` مورد نظر ایجاد نماییم.

* `Master` یا `Primary`: به سروری گفته می‌شود که اطلاعات خود را مستقیماً از فایل‌های `zone` موجود در دستگاه کسب می‌نماید.

* `Slave` یا `secondary`: به سروری گفته می‌شود که اطلاعات خود را از طریق سرورهای دیگر و در زمان `Zone transfer` دریافت می‌کند.

* `Zone transfer`: در صورت هر گونه تغییری در اطلاعات مربوط به یک `zone` بر روی `master` برای اطلاع `slave`ها یک انتقال `zone` صورت می‌گیرد.

* `Forward DNS`: وظیفه این `DNS`ها برگرداندن آدرس `IP` مربوط به نام یک `Host` می‌باشد.

* `Reverse DNS`: وظیفه این `DNS`ها برگرداندن نام `Host` معادل یک آدرس `IP` می‌باشد.

* اطلاعات `DNS`های مستقیم و معکوس (`Forward & Reverse`) بایستی منطبق باشند. اگر آدرس `IP` یک `Host` تغییر کرد باید این تغییر در فایلهای اطلاعاتی مرتبط با `Forward` و `Reverse zone` اعمال شود و شماره سریال هر فایل افزایش یابد. عدم همزمانی و تطابق این دو فایل باعث بروز مشکلاتی خواهد شد.

* دامنه `IN-ADDR. ARPA`: تمامی تبدیلهای معکوس (تبدیل آدرس به نام) در این `Domain` موجود است.

* `Named`: برنامه‌ای که لازم است به منظور انجام پرس و جوها بر روی `DNS server` نصب شود. اگر

`Named` نتواند به یک پرس وجو پاسخ دهد آنرا به `server` دیگری می‌فرستند و در طی این عمل، `Zone`

`transfer` انجام می‌شود، `Zone transfer` روشی است که اطلاعات تغییر کرده `DNS`ها را در اینترنت انتشار



Ahoo Engineering Group

می‌دهد. اگر برنامه Named در زمان نصب Redhat نصب نشده باشد آنرا از آدرس <http://www.redhat.com> یا CD نصب می‌کنیم.

نام فایل این نرم افزار، `bind-<version>.i386.rpm` می‌باشد. برای نصب این نرم افزار از دستور زیر استفاده می‌کنیم.

```
Rpm -ivh bind-<version>.i386.rpm
```

برای فعال و غیر فعال کردن سرویس named به صورت دستی از دستورات زیر استفاده می‌شود.

```
/etc/rc.d/init.d/named start
```

```
/etc/rc.d/init.d/named stop
```

و برای اجرای مجدد سرویس از دستورات زیر استفاده می‌شود.

```
/etc/rc.d/init.d/named reload
```

بعد از اعمال هر گونه تغییرات در فایل `/etc/named.conf` یا فایل‌های حاوی اطلاعات باید، این سرویس را مجدداً اجرا نمود.

* فایل `/etc/host.conf`: محتویات این فایل، ترتیب جستجوی آدرس IP یک دستگاه را تعیین می‌کند. و در اینجا نمونه‌ای از محتویات این فایل را آورده‌ایم:

```
Order host,bind
```

مفهوم عبارت بالا این است که برای جستجوی آدرس مربوط به یک دستگاه، ابتدا فایل `/etc/hosts` کنترل شود و در صورت عدم وجود نام و آدرس IP آن `host`، عمل پرس و جو از طریق DNS‌های موجود در فایل `/etc/resolv.conf` انجام شود. عمل جستجو در `/etc/host` خیلی سریع است زیرا اطلاعات این فایل بر روی همان دستگاه قرار دارد. در صورتی که DNS شبکه دچار مشکل شود خود دستگاه می‌تواند سریعاً آدرس IP معادل نام `host` مقصد را با خواندن محتویات فایل `/etc/hosts` پیدا کند.



Ahoo Engineering Group

* فایل `/etc/resolv.conf`: هر دستگاه داخل شبکه، یک DNS client است و برای اینکه بفهمد عمل جستجو

را توسط کدام DNS باید انجام دهد از اطلاعات این فایل استفاده می کند.

در اینجا نمونه ای از محتویات این فایل را آورده ایم:

```
domain domain.com
```

```
nemeserver 192.168.42.1
```

```
nameserver 192.168.42.2
```

سطر اول تعیین کننده نام Domain پیش فرض برای جستجوی می باشد. یعنی پرس و جوی آدرس IP

دستگاه host1 معادل تقاضای آدرس IP دستگاه host1.domain.com در نظر گرفته می شود. در این فایل

اجاره تعریف آدرس IP حداکثر سه سرور DNS را داریم.

Nslookup

بعد از نصب سرور DNS برای بررسی صحت عملکرد سرور از این دستور بر روی سرور و یا client استفاده

می شود. با اجرای این دستور به همراه یک پرامتر خاص که می تواند آدرس IP یا نام یک host باشد و

فرستادن این تقاضا به سرور، از سرور می خواهیم با جستجوی اطلاعات خود، پاسخ را ارسال نماید. به عنوان

مثال با فرض اینکه مشخصات دستگاهی با نام host1.domain.com بر روی سرور تعریف شده باشد، دستور

زیر را برای جست و جوی آدرس IP این دستگاه اجرا می نماییم:

```
nslookup host1.domain.com
```

در نتیجه در صورت عملکرد صحیح سرور بایستی پاسخی به شکل زیر دریافت نماییم.

```
Server:numrk.domain.com
```

```
Address:192.168.42.1#53
```

```
Name: host1.domain.com
```

```
Address:192.168.42.2
```

در صورت اجرای دستور بالا در یک client، تقاضای داده شده به اولین سرور تعریف شده در فایل

`/etc/resolv.conf` فرستاده می شود. حال اگر بخواهیم عملکرد دومین DNS موجود در فایل



Ahoo Engineering Group

etc/resolv.conf را بررسی کنیم چه باید کرد؟ در این مواقع، می‌توانیم با تایپ پارامتر دوم در مقابل

دستور nslookup که همان IP سرور مورد نظر می‌باشد، عملکرد سرور مورد نظر را بررسی نماییم.

در مثال زیر، آدرس IP دستگاه host1.domain.com از سروری که IP آن 192.168.42.1 می‌باشد

پرسیده می‌شود.

```
nslookup host1.domain.com 192.168.42.1
```

خروجی دستور فوق به صورت زیر می‌باشد:

```
Server: 192.168.42.1
```

```
Address:192.168.42.1#53
```

```
Name: host1.domain.com
```

```
Address:192.168.42.4
```

دو سطر اول نام و پورت سرور را تعیین می‌کند و دو سطر بعد نتیجه جستجو را که شامل نام و آدرس IP

میزبان می‌باشد، مشخص می‌نماید.

Traceroute

برای بررسی وضعیت مسیر طی شده توسط یک بسته تا رسیدن به مقصد از این دستور استفاده می‌شود.

این دستور به صورت کلی زیر استفاده می‌شود:

```
traceroute Destination_Address
```

که منظور از Destination_Address، نام یا آدرس IP مقصد می‌باشد. دستور مشابهی در clientهای ویندوزی

وجود دارد با این تفاوت که به جای دستور traceroute از دستور tracert استفاده می‌شود. Traceroute

بوسیله پروتکل ICMP (همانند ping) در مسیر رسیدن به مقصد هر ماشین را جستجو کرده و نام و آدرس IP

آنها می‌یابد.

در جواب اجرای این دستور، قبل از هر روتر موجود در مسیر، یک عدد نوشته شده که نمایانگر فاصله آن

host تا مقصد به صورت hop می‌باشد. تعداد hopها تا یک host نشانگر تعداد ماشینهای میانی است که باید



Ahoo Engineering Group

بسته را عبور دهند. اگر در خروجی دستور به جای نام host، علامت * ظاهر شود به این معنی است که آن host، بنا به دلایلی که عمده‌ترین آنها، قطعی شبکه و محافظتهای امنیتی Firewall می‌باشد، غیر قابل دسترسی است. همچنین با این دستور می‌توان به میزان اتصالات انجام شده تا یک سایت پی برد.

فایل `/etc/hosts`: اگر چه DNS اولین وسیله برای تحلیل نامهاست اما هنوز هم فایل `/etc/hosts`: روی اکثر کامپیوترها تعریف می‌شود که می‌تواند موجب سرعت بخشیدن به پرس و جوهای متناوب به منظور یافتن آدرسهای IP مربوط به local host شود. نمونه‌ای از فایل `/etc/hosts`: در اینجا آورده شده است.

به عنوان مثال در سطر اول بیان شده است که آدرس IP معادل دستگاه یا اصطلاحاً localhost، 127.0.0.1 می‌باشد و یا در سطر دوم بیان شده است که آدرس IP دستگاه localhost، 192.168.42.7 و نام مستعار این دستگاه، www می‌باشد.

#IP address	Hostname	Aliases
127.0.0.1	local host	
192.168.42.7	host1	www
192.168.42.8	mailhub	mailhub.domain.com
192.168.42.6	host2	

مراحل نصب یک Forward DNS Server

فرض کنیم نام Domain اختصاص داده شده، به ISP، domain.com باشد. حال قصد داریم برای تعریف مشخصات hostهای موجود در شبکه، یک DNS Server نصب نماییم. آدرس IP سرور را 192.168.42.1 در نظر می‌گیریم. هر DNS Server، از آدرس IP خود برای پاسخ به تقاضاها استفاده می‌نماید. لذا لازم است آدرس IP خود دستگاه را به عنوان اولین name server در فایل `/etc/hosts` تعریف کنیم. ضمناً برای پاسخ به تقاضاهایی که فقط نام host را بدون ذکر نام domain استفاده می‌کنند بهتر است نام domain پیش فرض نیز در این فایل تعریف شود.



Ahoo Engineering Group

محتوای فایل /etc/resolv.conf را به صورت زیر تغییر می‌دهیم :

```
domain    domain.com
```

```
name server 192.168.42.1
```

این فایل برای پیکربندی clientها (تقاضاها) استفاده می‌شود نه server خط اول، domain.com را به عنوان

نام دامنه پیش فرض برای client تعریف می‌کند و این دامنه‌ای است که به اسامی ماشینها ملحق می‌شود. خط

دوم، آدرس IP سروری است که به وسیله client استفاده می‌شود.

برای شروع تنظیمات سرور DNS نیاز به ویرایش فایل /etc/named.conf داریم. به نمونه اولیه‌ای از

محتویات این فایل که در زیر آمده است توجه کنید.

```
//generated by named-bootconf.pl
```

```
Options {
```

```
directory"/var/named";
```

```
/*
```

```
If there is firewall between you and nameservers you want
```

```
* to talk to, you might need to uncomment the query-source
```

```
* directive below. Pervious versions of BIND always asked
```

```
* questions using port 53, but BIND 8.1 uses an unprivileged
```

```
* port by default.
```

```
*/
```

```
// query-source address * port 53;
```

```
};
```

```
//
```

```
// a caching only nameserver config
```

```
//
```

```
Controls {
```

```
inet 127.0.0.1 allow {localhost; } keys {mdckey; } ;
```

```
};
```



```
zone "." IN{  
  
type hint;  
file "named.ca";  
};  
  
zone "localhost" IN{  
type master;  
file " localhost.zone";  
Allow-update {none; };  
};  
  
zone "0.0.127. in-addr.arpa"IN{  
type master;  
file " named.local";  
Allow-update {none; };  
};  
  
Include "/ect/rndc.key";
```

با توجه به محتویات فایل لیست شده بالا به هر یک از موارد زیر توجه کنید.

* یکی از پارامترهایی که در بخش options استفاده می شود عبارت directory است که برای تعیین مسیر فایل های اطلاعاتی مربوط به host های شبکه است و معمولا به طور پیش فرض از مسیر /var/named استفاده می شود.

* تمام فایل های اطلاعات zone در /uar/named/named.ca موجود است.

* ناحیه "." ، ریشه درخت DNS است یعنی مطالبی که در فایل named.ca قرار دارند لیستی از root serverها هستند.

* هر آدرس IP موجود در زیر شبکه 127.0.0.1 طبق اطلاعات مربوط به ناحیه و فایل named.local که توسط DNS استفاده می شود تحلیل می شود.



Ahoo Engineering Group

در زمان کار با فایل named.conf در نحوه تایپ علائم دقت داشته باشید . حال قصد داریم اطلاعات hostهای

داخل Domain شبکه‌مان را وارد کنیم. مراحل کار عبارتند از:

* تعریف ناحیه‌ای با نام Domain خودمان در فایل etc/named.conf اضافه می‌نماییم.

```
zone " domain.com" {
```

```
Type master;
```

```
file "named.domain.com"
```

```
};
```

مرحله دوم کار، تعریف مشخصات hostهای دامنه تعریف شده، در فایل /var/named/

named.domain.com می‌باشد. برای راحتی کار، یک کپی از فایل named.local /var/named/ با نام

named.domain.com در مسیر /var/named ایجاد کرده، سپس محتویات آنرا به دلخواه ویرایش می‌کنیم.

در ادامه نمونه‌ای از این فایل را توضیح می‌دهیم.

```
@ IN SOA numark.domain.com hostmaster.numarkdomain.com
```

```
1997022703 ;serial
```

```
28800 ;refresh
```

```
14400 ;retry
```

```
3600000 ; expire
```

```
86400) ; minimum
```

```
@ IN NS numark
```

```
@ IN MX 10 numark
```

```
numark IN A 192.168.42.1
```

```
mail IN A 192.168.42.2
```

```
www IN CNAME numarkdomain.com
```

فرمت هر خط در فایل اطلاعات zone

فرمت کلی پارامترهای این فایل به شکل زیر می‌باشد.

```
name IN record-type data
```



Ahoo Engineering Group

name: نمایانگر نام host می باشد که اگر با نقطه پایان نگیرد نام Domain در انتهای آن قرار می گیرد.

IN: این پارامتر به named می گوید که از کلاسهای اینترنت استفاده می کند.

record-type: نوع رکوردی را تعیین می کند که یکی از ۸ نوع زیر است.

SOA	: Start of Authority
NS	: Name server
A	: Address Record
PTR	: Pointer Record
MX	: Mail exchanger
CNAME	: Cannonic Name
RP and txt	: The documentation entries

رکورد SOA

خط اول فایل به نام Domain شروع می شود. دامنه هایی که نوشتن نامشان سخت است با سمبل @ کد می شوند.

ستون بعد از SOA، تعیین کننده نام Primary name server

برای این domain است که نام سرور را در این قسمت می نویسم و آخرش ستون، آدرس email شخصی است که

مشکلات سرور به او ارسال می شود. اما به جای @، علامت نقطه قرار گرفته است.

خط دوم، شماره سریال است که با هر تغییری در این فایل باید آنرا افزایش دهیم تا secondaryها بدانند که چه

زمانی zone transfer انجام دهند. فرمت کلی شماره سریال به صورت زیر است:

شماره سریال: YYYY MM DD XX

بهتر است شماره سریال را براساس همین فرمت کلی تعیین کنیم تا بعد از هر تغییری بدانیم، آخرین تغییر در چه

تاریخی انجام شده است. دو رقم آخر برای تعیین چندمین تغییر در آن روز است؛ بنابراین این ۰ تا ۹۹ بازیابی و

اصلاح در یک روز امکان ناپذیر است.



Ahoo Engineering Group

سطر بعدی یعنی refresh rate به slave می‌گوید که هر چند وقت یکبار در اثر بروز مشکل و به منظور به روز رسانی تغییرات باید master را چک کنند.

سطر بعدی سرعت سعی مجدد، بر حسب ثانیه است؛ یعنی اگر slave سعی در برقراری ارتباط با master دارد در صورت عدم موفقیت بعد از چه زمانی مجدداً سعی کند.

سطر چهارم به secondary می‌گوید که اگر متصل به primary server نشد بعد از چه مدت زمانی، صرف نظر کند که یک یا دو هفته مقدار خوبی است.

پارامتر minimum به caching server می‌گوید که در صورت عدم اتصال به primary قبل از رها کردن اتصال چه مدت منتظر بمانند که ۵ الی ۷ روز مناسب است.

رکورد NS

برای تعیین هویت و مشخصات server name های داخل Domain از رکورد NS استفاده می‌شود.

```
@      IN      NS      ns1.domain.com.
```

```
@      IN      NS      ns2.domain.com.
```

اگر رکورد NS مستقیماً بعد از رکورد SOA قرار گیرد نیازی به فیلد name (ستون اول)

در رکوردهای DNS نداریم. اگر در انتهای نامشان. نگذاریم نام Domain به آن متصل شده و باعث بروز مشکل می‌شود. یعنی ns1.domain.com به علت نداشتن نقطه در انتهای نام به صورت زیر در نظر گرفته می‌شود.

```
ns1.domain.com= ns1.domain.com.domain.com
```

رکورد A

رکورد آدرس، برای تبدیل نام سرور به IP مورد استفاده قرار می‌گیرد. به ازای هر ماشینی که نیاز به تحلیل نام و آدرسش باشد باید یک رکورد A در این فایل داشته باشیم. به مثال زیر توجه کنید:

```
mtx      IN      A      192.168.42.2
```



Ahoo Engineering Group

در مثال بالا چون در انتهای نام میزبان نقطه نگذاشته‌ایم اینطور در نظر گرفته می‌شود که دارای Domain

یکسانی با رکورد SOA است.

رکورد MX (mail exchanger)

این رکورد برای تعریف سروری در شبکه به عنوان مسئول دریافت mailها استفاده می‌شود. سرویس

Sendmail از این رکورد برای تشخیص ماشینی که باید mailهای رسیده به Domain را تحویل گیرد استفاده

می‌کند.

```
domain.com.      IN      MX      10      mailub
```

```
domain.com.      IN      MX      50      mailub2
```

ستون اول نام سروری است که mail به آدرسش ارسال شده، در ستون بعد از MX نشان دهنده سطح اولویت

است؛ اعداد کوچکتر نمایانگر اولویت بالاتر هستند. در مثال بالا اگر نامه‌ای با آدرس user1@domain.com

برای تعیین آدرس IP به DNS برسد، چون mailhub اولویت بالتری دارد، در نتیجه نامه به سمت

mailhub.domain.com

هدایت می‌شود و بایستی user1 جزء کاربران این دستگاه باشد. در صورتی که میزبان mailhub جواب ندهد.

نامه به سمت میزبانی با اولویت کمتر، یعنی mailub2 هدایت می‌شود.

رکورد CNAME (Canonical Name)

با این رکورد می‌توانیم برای hostها نام مستعار (Aliases) تعریف کنیم. قبل از تعریف نام مستعار، حتماً

بایستی، برای سرور مورد نظر، یک رکود A تعریف شده باشد که نام واقعی آنرا مشخص کنیم. به دستور زیر

که نام مستعاری برای mtX تعریف می‌کند توجه کنید.

```
IN      CNAME  mtX
```

در این مثال با فرض اینکه نام domain شبکه domain.com باشد،

www.domain.com به عنوان نام مستعاری برای mtX.domain.com توسط رکورد A تعریف شده است.



Ahoo Engineering Group

رکورد txt and PR

این رکورد برای تعریف اطلاعات اضافی مانند آدرس، تلفن و مسئول پاسخگویی استفاده می‌شود. این اطلاعات، نه فقط به شکل comment و توضیحات، بلکه به شکل رکوردهای واقعی که می‌توانند به وسیله دیگران استفاده شوند، مورد استفاده قرار می‌گیرند. رکوردهای txt از نظر فرم ظاهری نوشتن آزاد هستند و به هر شکلی می‌توان اطلاعات را وارد کرد.

```
domain.com. IN txt "contact : heidis."  
voice : (800) "@ IN txt "system Admin steator/ring master"  
@ IN txt "555-212"
```

رکورد RP به طور صریح مشخص می‌کند چه فردی به میزبانهای مشخص شده پاسخ می‌دهد.

```
domain.com. IN RP hidis.domain.com. domain.com.
```

و با تایپ آدرس email تعریف شده در رکورد SOA، شخص مورد نظر را به عنوان مسئول domain تعیین می‌کنیم.

بعد از ایجاد فایل حاوی اطلاعات Zone نوبت به آزمایش سرور می‌رسد.

ابتدا با اجرای دستور زیر سرویس named را مجدداً فعال می‌کنیم تا تغییرات ایجاد شده را اعمال نماید.

```
/etc/rc.d/init.d/named reload
```

سپس با اجرای دستور nslookup، پرس و جوهای مورد نظر را انجام می‌دهیم. برای درک بهتر مطلب به

مثالهای زیر توجه کنید.

```
nslookup mtz.domain.com  
nslookup mtz  
nslookup mtz 192.168.42.1  
nslookup www  
nslookup mailhub
```



Ahoo Engineering Group

اگر این پرس و جوها را بر روی سرور انجام دهیم، خود سرور به عنوان Client اقدام به انجام پرس و جوها می‌کند. یعنی از اطلاعات فایل `/etc/resolv.conf` برای پیدا کردن نام `name server` استفاده می‌نماید و بعد تقاضا را به آن میزبان می‌فرستند. در مثالهای بالا آدرس خود سرور در فایل `/etc/resolv.conf` به عنوان `name server` تعریف شده است. بنابراین نیازی به نوشتن نام `name server` به عنوان پارامتر دوم دستور `nslookup` نمی‌باشد.

در صورتی که در فایل `/etc/resolv.conf` نام دامنه پیش فرض نوشته نشده باشد، دستور دوم با مشکل مواجه خواهد شد.

دستور سوم در مواقعی استفاده می‌شود که در صورت وجود چندین `name server` در شبکه، بخواهیم پرس و جوی مورد نظر، صریحاً توسط `name server` خاصی پاسخ داده شود. در اینحالت باید آدرس IP آن `name server` را به عنوان پارامتر دوم دستور ذکر کنیم. بعد از اطمینان از عملکرد صحیح سرور می‌توانیم با میزبان‌های موجود در شبکه از طریق نام آنها ارتباط برقرار کنیم. مثلاً برای اطمینان از ارتباط دستگاه خود با `mailhub` از دستور زیر استفاده می‌کنیم.

```
Ping mailhub
```

مراحل نصب یک Reverse DNS Server

هدف از داشتن یک Reverse DNS پاسخ به تقاضاهای رسیده مبنی بر پرس و جوی نام یک میزبان با دادن IP میزبان می‌باشد. با فرض اینکه دامنه IP اختصاص داده شده به شبکه، `192.168.42` باشد مراحل زیر را انجام می‌دهیم.

* تعریف ناحیه‌ای در فایل `/etc/named.conf` و تعیین نام فایل حاوی آدرس میزبانهای شبکه.

* ایجاد فایل حاوی اطلاعات میزبانها در مسیر تعیین شده در فیلد `directory` از فایل `/etc/named.conf` که معمولاً `/var/named` می‌باشد.



Ahoo Engineering Group

* اجرای مجدد سرویس named

* انجام پرس و جویی برای بررسی عملکرد سرور.

برای انجام مرحله اول کار بخشی مانند زیر در فایل /etc/named.conf اضافه می‌نماییم.

```
zone "42.168.192.IN-ADDR.ARPA" {  
type master;  
file "named.192.168.42";  
};
```

در تعریف نام ناحیه، دامنه IP شبکه خود را به صورت معکوس، یعنی به صورت 42.168.192.IN-

ADDR.ARPA استفاده می‌نماییم.

مرحله دوم کار تعریف مشخصات hostهای دامنه تعریف شده، در فایل /var/named/named.192.168.42

می‌باشد. برای راحتی کار، یک کپی از فایل /var/named/named.local با نام named.192.168.42 در مسیر

/var/named ایجاد کرده / سپس محتویات آنرا به دلخواه ویرایش می‌کنیم.

در ادامه نمونه‌ای از این فایل را توضیح می‌دهیم.

```
@ IN SOA numark.domain.com hostmaster.numarkdomain.com.(
```

```
1997022703 ; serial
```

```
28800 ;refresh
```

```
14400 ;retry
```

```
3600000 ; expire
```

```
86400) ; minimum
```

```
@ IN NS numark.domain.com
```

```
1 IN PTR numark.domain.com
```

نکته ۱: نقطه گذاری در تمام فایل‌های DNS ضروری است. نام میزبانی که با "." خاتمه یابد کامل است؛ در غیر

این صورت به اثنهای نام آن، دامنه‌ای که با @ مشخص شده ملحق می‌شود.



Ahoo Engineering Group

نکته ۲: بعد از هر گونه تغییر در فایل‌های اطلاعات نواحی باید شماره سریال آن افزایش یابد و در انتها با دستور زیر، سرویس named را مجدداً اجرا می‌کنیم.

```
/ect/rc.d/init.d/named restart
```

رکورد PTR (Pointer Record)

این رکورد به Reverse resolution (تحلیل معکوس) نیز معروف است که به named می‌گوید چگونه نام معادل یک آدرس IP را برگرداند. این رکورد کمی با رکورد A فرق می‌کند. مثلاً در اینجا آدرس IPها معکوس است که در زیر شبکه In-addr.arpa هستند. به مثال زیر توجه کنید:

```
2.42.168.192. IN PTR mtz.domain.com.
```

برای آزمایش کردن Reverse DNS دستور زیر را اجرا می‌کنیم.

```
nslookup 192.168.42.1 192.168.42.1
```

اولین آرگومان، آدرس کامپیوتر مورد نظر برای جستجو و دومین آرگومان، آدرس IP مربوط به DNS است. دستور بالا باید خروجی زیر را تولید کند.

```
Server:numark.domain.com
```

```
Address: 192.168.42.1
```

```
Name:numark.domain.com
```

```
Address: 192.168.42.1
```

اگر خروجی، در عرض ۱ ثانیه تولید شود Reverse DNS در حال کار کردن است.

ایجاد زیر شبکه و هویت دادن به نمایندگان^۱

با وجود میلیون‌ها نام Domain و url روی اینترنت تنها راه نگهداری زنجیره ارتباطی، استفاده از یک سیستم

توزیع شده است. DNS از طریق هویت دادن به نمایندگان خود، این کار را می‌کند.



Ahoo Engineering Group

قصد داریم شبکه خود را به یک زیر شبکه جدید به نام subdomain تقسیم کنیم و مدیریت اسامی میزبانهای موجود در این زیر شبکه را به یکی از میزبانهای این زیر شبکه دهیم. جدول زیر لیست مشخصات چهار میزبان موجود در این زیر شبکه است.

IP	Host
192.168.42.40	Slvia
192.168.42.41	Brett
192.168.42.42	Rena
192.168.42.43	valeria

اسم کامل میزبانها به صورت زیر است:

sylvia.subdomain.domain.com

brett.subdomain.domain.com

rena.subdomain.domain.com

valerie.subdomain.domain.com

می‌خواهیم سرور sylvia را به عنوان Name server برای زیر شبکه subdomain.domain.com تعریف

کنیم. مراحل کار به صورت زیر می‌باشد که هر مورد را به صورت مجزا توضیح خواهیم داد:

* تعریف هویت زیر شبکه subdomain.domain.com روی sylvia

* آزمایش شناسایی میزبانهای داخلی زیر شبکه subdomain.domain.com

* تعریف نمایندگی sylvia به عنوان Name server زیر شبکه جدید، بر روی ماشین numark که Name

server اصلی شبکه است.

* آزمایش شناسایی نمایندگی subdomain.domain.com

تعریف هویت زیر شبکه subdomain.domain.com روی sylvia

برای تعریف ناحیه‌ای برای زیر شبکه subdomain.domain.com، خطوط زیر را ه فایل /etc/named.conf

در میزبان sylvia اضافه می‌کنیم.

```
zone " subdomain.domain.com" {
```

```
type master;
```

```
file " named.subdomain.domain.com";
```



Ahoo Engineering Group

;}}

سپس فایل حاوی اطلاعات میزبانهای این ناحیه را با نام `named.subdomain.domain.com` در مسیر

`/var/named` بر روی ماشین `sylvia` ایجاد می‌کنیم. در اینجا نمونه‌ای از محتویات این فایل را نمایش می‌دهیم.

```
@ IN SOA sylvia.subdomain.domain.com. hostmaster.subdomain.domain.com.(
```

```
1997022700 ; serial
```

```
28800 ;refresh
```

```
14400 ;retry
```

```
3600000) ; minimum
```

```
@ IN NS sylvia.subdomain.domain.com.
```

```
sylvia IN A 192.168.42.40
```

```
brett IN A 192.168.42.41
```

```
rena IN A 192.168.42.42
```

```
valerie IN A 192.168.42.43
```

سپس با دستور زیر سرویس `named` را در `sylvia` restart می‌کنیم.

```
/ect/rc.d/init.d/named restart
```

آزمایش شناسایی میزبانهای داخلی زیر بشکه `subdomain.domain.com`

برای اطمینان از عملکرد DNS Server تعریف شده بر روی `sylvia` و شناسایی میزبانهای موجود در این زیر

شبکه، دستورات زیر را اجرا می‌نماییم.

```
ping sylvia.subdomain.domain.com
```

```
ping brett.subdomain.domain.com
```

```
ping rena.subdomain.domain.com
```

```
ping valerie.subdomain.domain.com
```

نتایج اجرای دستورات بالا باید نشاندهنده آدرس IP صحیح باشد. اگر تحلیل نام `sylvia` به آدرس IP آن

موفقیت آمیز بود به نمایندگی گرفتن از `numark` می‌رسد.

تعریف نمایندگی `sylvia` در میزبان `numark`



Ahoo Engineering Group

در ماشین numark دو خط زیر را بعد از اتمام خطوط NS در فایل `/var/named/named.domain.com` اضافه می‌کنیم.

```
subdomain      IN      NS      sylvia.subdomain.domain.com.
```

```
sylvia.subdomain  IN      A       192.168.42.40
```

این دو خط بیان می‌کند که `sylvia.subdomain.domain.com` با IP داده شده، یک name server برای ناحیه `subdomain.domain.com` است. خط دوم برای تحلیل داخلی نام ارجاعی به `brett`، `rena` و `Valerie` وجود ندارد و این کار توسط `sylvia` صورت می‌گیرد و این زیبایی نمایندگی دادن به name serverهای دیگر است.

برای اتمام کار شماره سریال را افزایش داده و فایل را ذخیره کرده و `named` را مجدداً اجرا می‌کنیم.

آزمایش شناسایی نمایندگی `subdomain.domain.com`

بر روی ماشین `numark` سعی در `ping` نمودن به `sylvia.subdomain.domain.com` می‌کنیم در صورت مشکل، فایل `named.domain.com` را تست می‌کنیم. اگر موفق به `ping` شدیم، سعی در `ping` کردن به `brett.subdomain.domain.com` می‌نماییم. اگر این کار را از طریق `numark` انجام نشد آنرا از طریق `sylvia` انجام می‌دهیم. زمانی که توانستیم از طریق `numark` تمام `ping`ها را به چهار میزبان موجود در زیر شبکه انجام دهیم می‌فهمیم نمایندگی DNS درست انجام شده است.

Slave DNS server

اینترنت بدون وجود `Slave server`ها محل خوشایندی نخواهد بود. `Slave`ها اطلاعات خود را مستقیماً از `master` و یا از یک `slave` دیگر که مستقیماً اطلاعاتش را از `master` می‌گیرد، دریافت می‌نمایند. بنابراین می‌توانیم تعداد زیادی از `slave`ها را فقط با یک `master` مدیریت کنیم.

روال دریافت اطلاعات، `Zone Transfer` نامیده می‌شود این انتقالات در دو زمان صورت می‌گیرد:

* زمان `refresh` آن ناحیه فرا برسد.



Ahoo Engineering Group

* slave به عنوان یک رکورد NS موجود در رکوردهای نواحی master مورد مراجعه قرار گیرد و قسمت

options در فایل named.conf شامل notify نباشد.

مدیر سیستم، رکورد master zone را تغییر می‌دهد، شماره سریال را افزایش داده و named را مجدداً اجرا

می‌کند که این کار NOTIFY خوانده می‌شود.

توجه: NOTIFY فقط با masterها و slaveهای BIND8 کار می‌کند.

لازم به ذکر است که slave serverها اطلاعات خود را از master می‌گیرند، آنها را روی دیسک می‌نویسند،

بنابراین در صورت پایین رفتن master می‌توانند سرورهای DNS را مهیا کنند.

در این قسمت یک slave DNS server برای domain.com و محدوده 42.168.912 (DNS معکوس)

روی میزبان mtz ایجاد خواهیم کرد.

مراحل کار

۱. در فایل /ect/named.conf بر روی ماشین mtz، نواحی domain.com و Arpa 42.168.192.in-addr.

را ایجاد می‌کنیم.

۲. در ماشین mtz، سرویس named را restart می‌کنیم.

۳. در ماشین numark در فایل named.domain.com، ماشین mtz را به عنوان یک second name

server اضافه می‌کنیم.

۴. در ماشین numark در فایل named.192.168.42، ماشین mtz را به عنوان یک second name

server اضافه می‌کنیم.

۵. در numark، سرویس named را restart می‌کنیم.

۶. انجام تستهای مورد نیاز.

در اینجا مراحل بالا را به تفصیل بیان می‌کنیم.



zone های زیر را به فایل /ect/named.conf در mtX اضافه می کنیم.

```
zone " 42.168.192.in-adde.arpa" {  
type slave;  
file " slave.192.168.42";  
masters {192.168.42.1};  
};  
zone "domain.com" {  
type slave;  
file " slave.domain.com";  
masters {192.168.42.1};  
};
```

عبارت file تعیین کننده نام فایلی است که اطلاعات بدست آمده از master را در آن می نویسد. این فایل پرس و جوها را پاسخ می دهد.

عبارت masters {192.168.42.1}; به فایل named می گوید که هر گاه زمان refresh رسید یا هرگاه با یک NOTIFY از 192.168.42.1 برخورد کرد اطلاعات را از 192.168.42.1 دریافت کند.

عبارت است از Type slave به named می گوید که این ناحیه اجازه انجام master zone برای کسب اطلاعات از 192.168.42.1 را دارد.

توجه کنید که فایلها با کلمه slave به جای کلمه named شروع می شود و این امکان برای مدیر فراهم می شود که تمام slave zone ها را با دو دستور زیر بازخوانی کند.

```
rm slave./*  
/ect/rc.d/init.d/named restart
```

بر خلاف فایلهای اطلاعات master zone، فایلهای اطلاعات slave zone به وسیله اشخاص دستکاری نمی شوند و می توانند به وسیله server دوباره ایجاد شوند.



Ahoo Engineering Group

یک بار که slave zone اضافه شدند به سادگی با دستور زیر آنرا شروع می کنیم.

```
/ect/rc.d/init.d/named restart
```

named فایل های اطلاعات slave zone را ایجاد خواهد کرد و در حقیقت همانند یک DNS server کار می کند مگر اینکه عبارات NOTIFY را دریافت کند. (هنوز master چیزی در مورد slave zone نمی داند). بنابراین نصب یک slave برای master بدون اینکه master چیزی بداند امکان پذیر است. این DNS به دلیل بار ترافیکی زیادی که برای master پیش می آید مناسب نمی باشد و master باید از تمام slave ها مطلع باشد. Master می تواند با محدود کردن server هایی که می توانند zone transfer را دریافت کنند در مقابل slave های بدون هویت، خودش را محفوظ کند. فقط یکی از عبارات زیر را در قسمت سراسری zone از named.conf قرار می دهیم.

```
allow-transfer {192.168.42.2;}; #only mtz can be slave
```

یا

```
allow-transfer {192.168.42.2;192.168.42.10;}; #both
```

```
transfer {192.168.42/24;}; #only hosts on sobnet
```

از وجود فایل های /var/named.slave.domain.com و /var/named/slave.192.168.42 مطمئن می شویم

و بررسی می کنیم که آیا دستورات زیر خروجی های مورد نظر را تولید می کنند یا نه؟

nslookup	numark	192.168.42.2
nslookup	mtz	192.168.42.2
nslookup	numark.domain.com	192.168.42.2
nslookup	mtz.domain.com	192.168.42.2
nslookup	192.168.42.1	192.168.42.2
nslookup	192.168.42.2	192.168.42.2

تغییرات numark

در فایل named.domain.com بعد از خط IN NS خط زیر را اضافه می کنیم:



Ahoo Engineering Group

@ IN NS mtX

قبل از ذخیره کار و خروج ، شماره سریال را افزایش می دهیم. حال در فایل 192.168.42.named این خط را اضافه می کنیم.

@ IN NS 192.168.42

ماشین mtX.domain.com آدرس 192.168.42 را دارد. دوباره از افزایش شماره سریال اطمینان حاصل می کنیم.

در انتها با دستور زیر named را در ماشین numark مجددا اجرا می کنیم.

```
/ect/rc.d/init.d/named restart
```

اضافه کردن رکورد NS که NOTIFY را قادر می سازد که به DNS server روی mtX فرستاده شوند موجب

می شود که server یک zone transfer را انجام دهد. رکورد NS جدید به mtX امکان می دهد که همانند یک

backup name server مورد استفاده قرار گیرد. برای بررسی کارکرد slave zone ها دستورات زیر را اجرا

می کنیم.

nslookup	numark	192.168.42.2
nslookup	mtX	192.168.42.2
nslookup	numark.domain.com	192.168.42.2
nslookup	mtX.domain.com	192.168.42.2
nslookup	192.168.42.1	192.168.42.2
nslookup	192.168.42.2	192.168.42.2

DNS slave ها، zone transfer و نماینده ها به DNS امکان سرویس دهی میلیونها URL را می دهد.

مدیریت سرورها از راه دور



Ahoo Engineering Group

منابع و مراجع :

۱. کتاب نصب و راه اندازی شبکه های کامپیوتری و سرویسهای اینترنتی با Red Hat Linux جهاد دانشگاهی

مشهد مولف : سید امین حسینی سنو- معصومه قهرمانی

۲. وب سایت رسمی شرکت لینوکس – www.redhat.com

گردآورنده : علی محمد حسینی