16 March 2007

By: Mihai Marinof, Linux Editor

TLD Animation

How to Host Your Own Domain with Bind9 on Ubuntu

Set-up A DNS server to host your domain or provide a DNS server to your LAN.

If you have ever registered a domain, you might have noticed that you were asked to enter the IP address of two name servers. Those name servers are basically two BIND(9) daemons, running as master and slave, on two different machines. This is a commonly used setup for hosting your own domain; in case one breaks, the other will continue to server your website, mail server and any other services you might run. However, this is an optional step and you don't need to follow it if you're only looking to provide a DNS server for your network.***INSTALLING BIND 9***Before we start, keep in mind that you'll need root privileges to install and configure bind. I prefer switching user to root and execute the commands, rather than using sudo so this guide will assume you do the same. Otherwise, add 'sudo' before every command.Moreover, for this guide, I'll use as an example the domain "linux.lan" and IP addresses "10.10.0.77 and 10.10.0.78". You'll have to replace them with your own.. Switching to user root in a terminal and check for updates:[CODE=0]$ sudo passwd rootPassword: (Enter the password for current user)Enter new UNIX password: (Enter the password you want to set for root)Retype new UNIX password: (Retype root password)passwd: password updated successfully$ su -Password: (Enter root password here)# apt-get update; apt-get upgrade[CODE=1]. Install BIND9:[CODE=0]# apt-get install bind9[CODE=1]***CONFIGURING BIND***. Ubuntu provides you with a pre-configured version of Bind so you will only have to open the file */etc/bind/named.conf.local* in your favorite editor and insert your zones. A zone is a domain name that is referenced in the DNS server.[CODE=0]zone "linux.lan" { type master; file "/etc/bind/zones/linux.lan.db"; };zone "0.10.10.in-addr.arpa" { type master; file "/etc/bind/zones/rev.0.10.10.in-addr.arpa";};[CODE=1]. Next, edit the bind options file, */etc/bind/named.conf.options* and modify the *forwarders* directive. This is the DNS server to witch your Bind installation will forward the requests it can't process. Replace the IP given as an example in that file with the DNS IP address provided by your ISP. Also, make sure the *forwarders* directive ISN'T commented out (has two slashes in front of it). If it does, remove them.. It's time to add the zone definition files. Create the zones directory: [CODE=0]# mkdir /etc/bind/zones[CODE=1]. Add the zone definitions to file */etc/bind/zones/linux.lan.db* (file does not exist, create it):[CODE=0]linux.lan. IN SOA ns1.linux.lan. admin.linux.lan. (2006081401 28800 3600 604800 38400)linux.lan. IN NS ns1.linux.lan. IN A 10.10.0.77mail.linux.lan. IN MX 10 mail.linux.lan.linux.lan. IN MX 10 mail.linux.lan.www IN A 10.10.0.77mail IN A 10.10.0.77ns1 IN A 10.10.0.77[CODE=1] . Create the reverse DNS zone file. Create the file */etc/bind/zones/rev.rev.0.10.10.in-addr.arpa* and add:[CODE=0]@ IN SOA linux.lan. admin.linux.lan. (2006081401; 28800; 604800; 604800; 86400); IN NS ns1.linux.lan.77 IN PTR linux.lan.[CODE=1]. Restart Bind so the changes will take effect:[CODE=0] # /etc/init.d/bind9 restart[CODE=1]***TESTING BIND***. To test DNS resolving, use either *host*, *dig*, both or any other tools (nslookup etc):[CODE=0]# host linux.lan 127.0.0.1linux.lan has address 10.10.0.7linux.lan mail is handled by 10 mail.linux.lan.[CODE=1][CODE=0]# dig linux.lan; QUESTION SECTION:;linux.lan. IN A;; ANSWER SECTION: linux.lan. 38400 IN A 10.10.0.77;; AUTHORITY SECTION:linux.lan. 38400 IN NS ns1.linux.lan.;; ADDITIONAL SECTION:ns1.linux.lan. 38400 IN

A 10.10.0.77[CODE=1]***CHANGING DEFAULT DNS SERVER***. If the results are similar to the ones above, it's time to make your system use the new DNS server. Edit the file */etc/resolv.conf* to look like:[CODE=0]search linux.lannameserver 10.10.0.77nameserver 123.123.123.123[CODE=1]Where 10.10.0.77 is the server's IP running Bind, which is also reachable by computers in your network or Internet (depending on what you want to do with your DNS server), and 123.123.123.123 is the DNS IP address provided by your ISP. ***INSTALLING SLAVE DNS SERVER***. On another machine, follow the same guide above until the ZONES part.- **The following commands are for the slave server unless stated otherwise.** -. Create the zones directory:[CODE=0]# mkdir /etc/bind/zones[CODE=1]. For **BOTH** master and slave, edit */etc/bind/named.conf.options* and add this line within the options section (somewhere in the middle of the file, not at beginning/end):[CODE=0] dnssec-enable yes;[CODE=1]. Use dnssec-keygen to generate a .private and .key file: [CODE=0]# dnssec-keygen -a hmac-md5 -b 128 -n host linux.lan[CODE=1]. Add this in your /etc/bind/named.conf on master **AND** slave. Open the .private file generated earlier and copy the hashkey from *Key*:, then paste it to secret directive:[CODE=0]key "TRANSFER" { algorithm hmac-md5; secret "HASHKEY-FROM-.PRIVATE-FILE";}; [CODE=1]. On the **MASTER** server, add the slave IP to */etc/bind/named.conf* (again, don't forget to replace the examples with your valid IP addresses):[CODE=0]server 10.10.0.78 { keys { TRANSFER; };};[CODE=1]. On the **SLAVE** server, add the master IP to */etc/bind/named.conf*:[CODE=0]server 10.10.0.77 { keys { TRANSFER; };}; [CODE=1]. Add the following to */etc/bind/named.conf.local* (yes, on slave):[CODE=0]zone "linux.lan" { type slave; file "/etc/bind/zones/slave_linux.lan.db"; masters { 10.10.0.77; }; allow-notify { 10.10.0.77; };};[CODE=1]. Finally, add this to */etc/bind/named.conf*:[CODE=0]include "/etc/bind/rndc.key";[CODE=1]When Bind will be restarted, there will be a zone transfer. This requires a synchronized clock, so the last step before restarting bind is to run the following command on both servers:[CODE=0]# apt-get -y install ntpdate[CODE=1]Enjoy!