Configuring RNDC for BIND9

Written by Admin
Tuesday, 04 September 2012 10:00 -

Configuring rndc for BIND 9 can be tricky. You need to first have a **rndc.conf** file created with a security key.

rndc-confgen -a -c /etc/namedb/rndc.conf -k dnsadmin -b 256

The **-k** option to set the key name that is generated by rndc-confgen to be something different than the default name of "rndc-key". It is highly recommended that you do change the key name, mostly on a DNS server that is on a network that you may not have full knowledge or control over the traffic flowing through it, mostly when you want to open up rndc use to other machines on that network.

The **-b** is option sets the key size, in bits, that is generated. By default, the key size is 128 bits, though the size can range from 1 to 512 bits. It is recommended that you use a key size of at least 256 bits if you are using this for a public DNS server.

This creates the **rndc.conf** file with this information.
key "rndc-key" {
algorithm hmac-md5;
secret "nm/hkdldjGjsdfjSdfsdDD==";
};

Add this to the file.
options {
default-key "rndc-key";
default-server 127.0.0.1;
};

Next you need to add the key info to the **namedb.conf** file.

key "dnsadmin" {
algorithm hmac-md5;
secret "secret-string";
};

controls {
*inet * allow { 127.0.0.1; } keys { "dnsadmin"; };*
};

Now, stop and restart your bind service.