

» **Contact HP**» **Large Enterprise Business**

- » Products
- » Business & IT services
- » Solutions

» **Open source & Linux**

- » Platforms & printers
- » Linux distributions
- » Indemnity
- » Support matrices
- » Security certifications
- » Solutions portfolio
- » HP Open Source Middleware Stacks
- » Documentation
- » Services & education
- » Open source at HP
- » Partner programs



search:

Open Source @ HP all of HP US

Open Source and Linux from HP

Primed for Business Advantage

HP TechBriefs



Configuring Secure Dynamic DNS in a Linux Environment by Jimmy Vance

This TechBrief provides information for configuring DHCP to automatically authenticate or update DNS data.

- » **Why the need for Dynamic DNS Configuration**
- » **Novell/SUSE Linux**
- » **Red Hat Linux**
- » **Troubleshooting**
- » **Example files**
- » **Summary**
- » **Acknowledgement**
- » **Footnotes**

Why the need for Dynamic DNS (DDNS)?

With the proper setup, DDNS can reduce your IP address-management workload and provide detailed and consistent information to the services on your network. You'll finally be able to update your name information dynamically while configuring your network with DHCP.

When configuring and deploying a blade server in a Linux only environment, accessing system setup or management can be a daunting task. With a new blade server in hand, identification of the blade is the iLO name. Utilizing DDNS, you can access iLO using the IP address without having to worry about the specific IP or MAC address (<http://ilo12345.example.com>).

Configuration

The ISC DHCP server v3 supports dynamic DNS updates (DDNS), as does BIND 9. These standards in the works. For now, the best way is to have the updates done by the DHCP server (not by the clients themselves).

Here is a short outline of how things work together:

- DHCP clients send their preferred hostname along with the request
- dhcpd acknowledges the lease
- dhcpd contacts named, asking it to update the zone, using an HMAC-MD5 key (Transaction Signature) for authentication
- named updates the zone (and rewrites the zone files periodically)
- when the lease times out or is freed, named will remove it

The following instructions should get you up and running. They are basically taken from `dnsmasq` and `dhcpd.conf` man pages. There are minor differences in configuration between Red Hat; I'll detail the configuration on both distributions. At the end of this document are complete example files for `dhcpd.conf`, `named.conf` and zone files that can be used for both distributions.

Novell/SUSE Linux

With SUSE Linux you can use the GUI tool, YaST to completely configure DHCP, DNS and DNSSEC. No manual editing of the configuration files is required. For those who prefer the command line method, we will step through the files for manual configuration.

The following packages need to be installed:

```
dhcp-3.* or later
dhcp-server-3.* or later
dhcp-tools-1.6* or later
bind-9.* or later
bind-utils-9.* or later
```

The following files will be created/modified:

```
/etc/dhcp.conf
/etc/named.conf
/etc/named.keys
```

```
/etc/named.conf.include
/etc/sysconfig/dhcp
/etc/sysconfig/named
```

Make a key to be used by dhcpd to authenticate for DNS updates. Use the script `/usr/bin/genDDNSkey`, which essentially runs BIND's key generating utility, extracts the `K*` private key file and puts it into the file `/etc/named.keys`. The file name and key specified on the command line, or via a shell environment.

Call `genDDNSkey --help` for usage info.

```
The simplest example is: genDDNSkey
which is equivalent to
genDDNSkey --key-file /etc/named.keys --key-name DHCP_UPDATER
```

Configure dhcpd:

`/etc/dhcpd.conf` needs these additional lines:

```
# /etc/dhcpd.conf
ddns-update-style interim;
ddns-updates on;
ignore client-updates;
include "/etc/named.keys";
```

and in the subnet declaration the addition of the zone directive:

```
#
subnet 192.168.1.0 netmask 255.255.255.0 {
range 192.168.1.100 192.168.1.250;
zone example.com. { primary 127.0.0.1; key DHCP_UPDATER; }
zone 1.168.192.in-addr.arpa. { primary 127.0.0.1; key DHCP_UPDATER;
}
```

The DHCP server runs in a chroot jail by default. The key file needs to be copied into the `dhcpd` cannot access files outside it. This can easily be achieved by adding `/etc/named` value of `DHCPD_CONF_INCLUDE_FILES` in `/etc/sysconfig/dhcpd`.

```
# /etc/sysconfig/dhcpd
DHCPD_INTERFACE="eth0"
#
DHCPD_RUN_CHROOTED="yes"
#
DHCPD_CONF_INCLUDE_FILES="/etc/named.keys"
#
DHCPD_RUN_AS="dhcpd"
```

Configure named: `Named.conf` needs to include the key, and to allow updates. Append along these lines to `/etc/named.conf`:

```
# /etc/named.conf

# named.keys is listed in the named.conf.include file
include "/etc/named.conf.include";

zone "example.com" in {
type master;
file "dyn/example.com";
allow-update { key DHCP_UPDATER; };
};

zone "1.168.192.in-addr.arpa" in {
type master;
file "dyn/1.168.192.in-addr.arpa";
allow-update { key DHCP_UPDATER; };
};
```

Instead of putting the include statement directly in `named.conf`, SUSE has a separate additional configuration files. Example `named.conf.include`

```
# /etc/named.conf.include

# Add additional configuration files which should be added to
#/etc/named.conf by this mechanism to NAMED_CONF_INCLUDE_FILES in
#/etc/sysconfig/named. This is possible with the YaSt sysconfig or
```

```
#any other editor.
include "/etc/named.keys";
```

Like dhcpd, named runs in a chroot directory, so we need to add /etc/named.keys to the NAMED_CONF_INCLUDE_FILES in /etc/sysconfig/named, just as we did with dhcpd.

```
# /etc/sysconfig/named
#
NAMED_RUN_CHROOTED="yes"
#
NAMED_CONF_INCLUDE_FILES="/etc/named.keys"
```

named runs, by default as user "named". named needs to create its .jnl files, but it is not allowed to do that in its working directory (/var/lib/named) for security reasons. named can create files in /var/lib/named/dyn so the file directive needs to have dyn/ as the leading path in named.conf.

As stated both dhcpd and named run in a chroot jail. The startup scripts for both services copy needed files into the chroot environment. This allows the configuration files to be kept where they would normally expect to find them.

Red Hat Linux (and most other Linux variants)

The following packages need to be installed:

```
dhcp-3.* or later
bind-9.* or later
bind-utils-9.* or later
bind-chroot-9.* or later
```

The following files will be created/modified:

```
/etc/dhcp.conf
/etc/named.keys
/var/named/chroot/etc/named.keys
/var/named/chroot/etc/named.conf
```

Red Hat, unlike SUSE, does not provide tools to create the TSIG key, or to configure DHCP. Red Hat runs named in a chroot jail, but not dhcp.

The following script creates named.keys, and puts it in the proper directories. The script also creates the directories for the dynamic zone files.

```
#!/bin/bash
#
# genDDNS-RH
#
# create TSIG key and setup dynamic zone directory
#
# find and set ROOTDIR variable
[ -r /etc/sysconfig/named ] && . /etc/sysconfig/named

export KEYFILE=named.keys
export KEYNAME=DHCP_UPDATER
export RANDOM_DEV=/dev/random

# go to chroot jail
cd ${ROOTDIR}/etc
keyfile=$(/usr/sbin/dnssec-keygen -a hmac-md5 -b 512 -r ${RANDOM_DEV} -n user $)

echo $keyfile

# read the secret
while read line; do
  case $line in
    Key:*) secret=${line#* }
    esac
done < $keyfile.private

cat >${KEYFILE} <<-EOF

# generated by $(basename $0) on $(date)

key ${KEYNAME} {
  algorithm hmac-md5;
  secret "$secret";
};
EOF
```

```
# set permissions and file locations
chown root:named $KEYFILE
chmod 644 $KEYFILE
cp -a ${ROOTDIR}/etc/named.keys /etc/named.keys

# create dynamic zone file location
if [ ! -d ${ROOTDIR}/var/named/dyn ]; then
  mkdir ${ROOTDIR}/var/named/dyn
  chown named:named ${ROOTDIR}/var/named/dyn
  chmod 770 ${ROOTDIR}/var/named/dyn
fi
```

Configure dhcpd:

/etc/dhcpd.conf needs these additional lines:

```
# /etc/dhcpd.conf
ddns-update-style interim;
ddns-updates on;
ignore client-updates;
include "/etc/named.keys";
```

and in the subnet declaration the addition of the zone directive:

```
#
subnet 192.168.1.0 netmask 255.255.255.0 {
  range 192.168.1.100 192.168.1.250;
  zone example.com. { primary 127.0.0.1; key DHCP_UPDATER; }
  zone 1.168.192.in-addr.arpa. { primary 127.0.0.1; Key DHCP_UPDATER; }
}
```

Configure named:

Named.conf needs to include the key, and allow updates. Append something along the /etc/named.conf:

```
# /etc/named.conf
include "/etc/named.keys";

zone "example.com" in {
  type master;
  file "dyn/example.com.zone";
  allow-update { key DHCP_UPDATER; };
};

zone "1.168.192.in-addr.arpa" in {
  type master;
  file "dyn/1.168.192.in-addr.arpa.zone";
  allow-update { key DHCP_UPDATER; };
};
```

named runs, by default as user "named". named needs to create its .jnl files, but it isn't do that in its working directory (/var/named) for security reasons. named can create a in /var/named/dyn so the file directive needs to have dyn/ as the leading path for the named.conf.

Troubleshooting

dhcpd and named will not operate properly if Security Enhanced Linux (SELinux) was installed on the operating system. This is because the SELinux policy role for dhcpd or named does not match the application usage for DDNS. By default, SELinux is disabled in SUSE and Red Hat. The simplest solution is to either disable SELinux or set the behavior to 'warn'. Alternatively you could create a SELinux policy role that matches the files, privileges, and named. Refer to your distribution's documentation as SELinux configuration is beyond the scope of this TechBrief.

Check /var/log/messages for other errors. Both DHCP and BIND log messages there and named will give the right clues to any problems.

Firewall rules must be modified to allow DHCP and DNS traffic. SUSE can be modified by editing the file, /etc/sysconfig/SUSEfirewall2. Red Hat can be modified using Security Editor by editing the file /etc/sysconfig/iptables

Example Files

A working dhcpd.conf file follows:

```
# /etc/dhcpd.conf
option domain-name "example.com";
option domain-name-servers 192.168.1.10;
option routers 192.168.1.1;
default-lease-time 86400;
authoritative;
ddns-update-style interim;
ddns-updates on;
ignore client-updates;
include "/etc/named.keys";
subnet 192.168.1.0 netmask 255.255.255.0 {
    range 192.168.1.100 192.168.1.250;
    zone example.com. { primary 127.0.0.1; key DHCP_UPDATER; }
    zone 1.168.192.in-addr.arpa. { primary 127.0.0.1; Key DHCP_UPDATER; }
}
```

Note that this example implies that the DNS server runs on the same machine (127.0.) easily be modified to point to the DNS server if it runs on another system.

A named.conf file for SUSE follows:

```
# /etc/named.conf
#
options {
    directory "/var/lib/named";
    dump-file "/var/log/named_dump.db";
    statistics-file "/var/log/named.stats";
    notify no;
    forwarders { 192.168.2.10; };
};

logging {
    category default { default_syslog; };
};

zone "." in {
    type hint;
    file "root.hint";
};

zone "localhost" in {
    type master;
    file "localhost.zone";
};

zone "0.0.127.in-addr.arpa" in {
    type master;
    file "127.0.0.zone";
};

include "/etc/named.conf.include";

zone "example.com" in {
    allow-transfer { localhost; localnets; };
    file "dyn/example.com";
    type master;
    allow-update { key DHCP_UPDATER; };
};

zone "1.168.192.in-addr.arpa" in {
    allow-update { key DHCP_UPDATER; };
    allow-transfer { localhost; localnets; };
    file "dyn/1.168.192.in-addr.arpa";
    type master;
};
```

A named.conf file for Red Hat follows:

```
#
# /etc/named.conf
#
options {
    directory "/var/named";
    dump-file "/var/named/data/named_dump.db";
```

```

statistics-file "/var/named/data/named.stats";
listen-on-v6 { none; };
notify no;
forwarders { 208.246.182.5; };
};

#controls {
#   inet 127.0.0.1 allow { localhost; } keys { rndckey; };
#};

zone "." IN {
    type hint;
    file "named.ca";
};

zone "localdomain" IN {
    type master;
    file "localdomain.zone";
    allow-update { none; };
};

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; };
};

zone "255.in-addr.arpa" IN {
    type master;
    file "named.broadcast";
    allow-update { none; };
};

zone "0.in-addr.arpa" IN {
    type master;
    file "named.zero";
    allow-update { none; };
};

include "/etc/named.keys";
include "/etc/rndc.key";

zone "example.com" in {
    allow-transfer { localhost; localnets; };
    file "dyn/example.com";
    type master;
    allow-update { key DHCP_UPDATER; };
};

zone "15.168.192.in-addr.arpa" in {
    allow-update { key DHCP_UPDATER; };
    allow-transfer { localhost; localnets; };
    file "dyn/15.168.192.in-addr.arpa";
    type master;
};

```

Forward zone file

```

$ORIGIN .
$TTL 172800 ; 2 days
example.com IN SOA lab.example.com. root.lab.example.com.
(
    2005110624 ; serial
    10800 ; refresh (3 hours)
    3600 ; retry (1 hour)
    604800 ; expire (1 week)
    86400 ; minimum (1 day)
)
NS ns1.example.com.
MX 0 mail.example.com.
$ORIGIN example.com.
ftp CNAME lab
lab A 192.168.15.21
mail CNAME lab
ns1 CNAME lab
www CNAME lab

```

Reverse zone file

```
$ORIGIN .
$TTL 172800 ; 2 days
15.168.192.in-addr.arpa IN SOA lab.example.com. root.lab.example.com
(
    2005110616 ; serial
    10800 ; refresh (3 hours)
    3600 ; retry (1 hour)
    604800 ; expire (1 week)
    86400 ; minimum (1 day)
)
    NS ns1.example.com.
    MX 0 20.15.168.192.in-addr.arpa.

$ORIGIN 15.168.192.in-addr.arpa.
21 PTR lab.example.com.
```

Summary

This TechBrief should provide you with enough information to properly configure and r Dynamic DNS. This provides a valuable foundation for simplified installation and mana servers.

Acknowledgement

Jimmy Vance is a Linux Technology Expert in the HP Linux Solution Alliances Engine The group works with a number of Linux-based ISVs to support various ProLiant and BI initiatives. See www.hp.com/go/ActiveAnswers for additional technical whitepapers an partner solutions. Jimmy has been using Linux at home and professionally since the m located in Houston, Texas.

Was this article useful? [Tell us what you think!](#)

 [Printable version](#)

[Privacy statement](#)

[Using this site means you accept its terms](#)

[Feedback to Webmaster](#)

© 2007 Hewlett-Packard Development Company, L.P.