



## Samba4 as AD domain controller on Centos 6

With the last version of samba 4 comes with Active directory logon and administration protocols, including typical active directory support and full interoperability with Microsoft Active Directory servers. This is possible with the combination of a LDAP directory, [heimdal kerberos](#) authentication, dynamic DNS server and the necessary remote procedure calls RPC. For complete list of the new changes you can see the next url: <http://wiki.samba.org/index.php/Samba4>



This post covers the initial installation and configuration of samba 4 as Active Directory domain controller, on Centos 6 using bind 9 as DNS backend and NTPD (4.2.6) server used by the clients.

– Change the hostname:

```
1 # vi /etc/sysconfig/network
2
3 HOSTNAME=centos-dc
```

– Disable selinux:

```
1 # vi /etc/sysconfig/selinux
2
3 SELINUX=disabled
4
```

### Categories

[AWS](#)

[Backup](#)

[Clustering](#)

[Database](#)

[DNS](#)

[GNU/Linux](#)

[Kernel](#)

[LDAP](#)

[Mail](#)

[Monitoring](#)

[Networking](#)

[Performance](#)

[Scripting](#)

[Security](#)

[Storage](#)

[Unix](#)

```
5 | # setenforce 0
```

– Install some dependencies:

```
1 | # yum -y install gcc make wget python-  
devel gnutls-devel openssl-devel libacl-  
devel krb5-server krb5-libs krb5-  
workstation bind bind-libs bind-utils
```

– Download and compile samba4:

```
1 | # wget  
2 | http://ftp.samba.org/pub/samba/samba-  
3 | latest.tar.gz  
4 | # tar -xzf samba-latest.tar.gz  
5 | # cd samba-latest/  
# ./configure --enable-selftest  
# make && make install
```

– Provisioning a new domain:

```
1 | # /usr/local/samba/bin/samba-tool domain  
provision --realm=opentodo.net --  
domain=OPENTODO --adminpass 'P@ssw0rd' --  
server-role=dc --dns-backend=BIND9_DLZ
```

The dns backend BIND9\_DLZ uses samba4 AD to store zone information

– Edit named configuration:

```
1 | # rndc-confgen -a -r /dev/urandom  
  
1 | # vi /etc/named.conf  
2 |  
3 | options {  
4 | listen-on port 53 { any; };  
5 | forwarders {192.168.1.8; };  
6 | allow-query { any; };  
7 | tkey-gssapi-keytab  
8 | "/usr/local/samba/private/dns.keytab";  
9 | };  
include  
"/usr/local/samba/private/named.conf";
```

– Edit resolv.conf:

```
1 | # vi /etc/resolv.conf  
2 |  
3 | nameserver 127.0.0.1  
4 | domain opentodo.net
```


Virtualization

Web

## Tags

AAA apache2 backup bandwidth  
barnyard2 base bind bind9 bind9  
logging centos compile  
corosync debian freebsd  
freeradius galera github  
heartbeat iptables iscsi  
ldap linux lvm make  
Monitoring multi-master  
multipath mysql nagios  
named NAT networking nfs  
nginx pacemaker perl  
postfix relay scripts snmp  
snort ssl tcp tls  
XenServer

## Github



**opentodonet**  
Ivan Mora Pérez  
Barcelona

21
Public Repos
3
Public Gists
15
Followers

 Follow @ivanimp91

 "Planet SysAdmin"

– Edit kerberos server configuration:

```
1 | # vi /etc/krb5.conf
2 |
3 | [libdefaults]
4 | default_realm = OPENTODO.NET
5 | dns_lookup_realm = false
6 | dns_lookup_kdc = true
```

– Download and install the last version of ntp (4.2.6 comes with ntp sign support):

```
1 | # wget
2 | http://www.eecis.udel.edu/~ntp/ntp_spool/ntp-
3 | 4.2/ntp-4.2.6p5.tar.gz
4 | # tar -xzf ntp-4.2.6p5.tar.gz
5 | # cd ntp-4.2.6p5
   | # ./configure --enable-ntp-sign
   | # make && make install
```

– Configuring NTP:

```
1 | # vi /etc/ntp.conf
2 |
3 | server 127.127.1.0
4 | fudge 127.127.1.0 stratum 10
5 | server 0.pool.ntp.org iburst prefer
6 | server 1.pool.ntp.org iburst prefer
7 | driftfile /var/lib/ntp/ntp.drift
8 | logfile /var/log/ntp
9 | ntpsigndsocket
10 | /usr/local/samba/var/lib/ntp_signd/
11 | restrict default kod nomodify notrap
12 | nopeer mssntp
13 | restrict 127.0.0.1
   | restrict 0.pool.ntp.org mask
   | 255.255.255.255 nomodify notrap nopeer
   | noquery
   | restrict 1.pool.ntp.org mask
   | 255.255.255.255 nomodify notrap nopeer
   | noquery
```

– Setting up the correct permissions:

```
1 | # chown named:named
2 | /usr/local/samba/private/dns
3 | # chown named:named
   | /usr/local/samba/private/dns.keytab
   | # chmod 775 /usr/local/samba/private/dns
```

– Configuring samba init script:

```
1 | # vi /etc/init.d/samba4
```

[Chris Siebenmann: Some notes on entering unusual characters in various X applications](#) December 30, 2015

---

[Anton Chuvakin - Security Warrior: Links for 2015-12-29 \[del.icio.us\]](#) December 30, 2015

---

[System Administration Advent Calendar: Day 25 - Laziest Christmas Ever](#) December 29, 2015

---

## "LinuxPlanet Blogs"

[I've Got A Date](#) December 25, 2015 *Dan*

---

[New Relic PHP Agent Issue with Laravel 5.2](#) December 23, 2015 *Mark Davidson*

---

[Conservancy's Year In Review 2015](#) December 18, 2015 *Bradley M. Kuhn*

---

```
1  #! /bin/bash
2  #
3  # samba4 Bring up/down samba4 service
4  #
5  # chkconfig: - 90 10
6  # description: Activates/Deactivates all
7  samba4 interfaces configured to
8  # start at boot time.
9  #
10 ### BEGIN INIT INFO
11 # Provides:
12 # Should-Start:
13 # Short-Description: Bring up/down samba4
14 # Description: Bring up/down samba4
15 ### END INIT INFO
16 # Source function library.
17 . /etc/init.d/functions
18
19 if [ -f /etc/sysconfig/samba4 ]; then
20 . /etc/sysconfig/samba4
21 fi
22
23 CWD=$(pwd)
24 prog="samba4"
25
26 start() {
27 # Attach irda device
28 echo -n "Starting $prog: "
29 /usr/local/samba/sbin/samba
30 sleep 2
31 if ps ax | grep -v "grep" | grep -q
32 /samba/sbin/samba ; then success "$samba4
33 startup"; else failure "$samba4 startup";
34 fi
35 echo
36 }
37 stop() {
38 # Stop service.
39 echo -n "Shutting down $prog: "
40 killall samba
41 sleep 2
42 if ps ax | grep -v "grep" | grep -q
43 /samba/sbin/samba ; then failure "$samba4
44 shutdown"; else success "$samba4
45 shutdown"; fi
46 echo
47 }
48 status() {
49 /usr/local/samba/sbin/samba --show-build
50 }
51
52 # See how we were called.
53 case "$1" in
54 start)
55 start
```

```

56 ;;
57 stop)
58 stop
59 ;;
60 status)
61 status irattach
62 ;;
63 restart|reload)
64 stop
65 start
  ;;
  *)
  echo $"Usage: $0
  {start|stop|restart|status}"
  exit 1
esac

  exit 0

```

```

1 | # chmod 755 /etc/init.d/samba4

```

- Configuring ntp init script:

```

1 | # vi /etc/init.d/ntp

```

```

1  #!/bin/bash
2  #
3  # ntp Bring up/down ntp service
4  #
5  #chkconfig: - 99 30
6  #description: Bring up/down ntp
7  #
8  ### BEGIN INIT INFO
9  # Provides:
10 # Should-Start:
11 # Short-Description: Bring up/down ntp
12 # Description: Bring up/down ntp
13 ### END INIT INFO
14 # Source function library.
15 . /etc/init.d/functions
16
17 CWD=$(pwd)
18 NTPD=/usr/local/bin/ntpd
19 prog="ntp"
20 start() {
21 # Attach irda device
22 echo -n "Starting $prog: "
23 $NTPD -p /var/run/ntpd.pid
24 sleep 2
25 if ps ax | grep -v "grep" | grep -q $NTPD
26 ; then success $"ntp startup"; else
27 failure $"ntp startup"; fi

```

```

28 | echo
29 | }
30 | stop() {
31 | # Stop service.
32 | echo -n $"Shutting down $prog: "
33 | kill -9 `cat /var/run/ntpd.pid` >
34 | /dev/null 2>&1
35 | sleep 2
36 | if ps ax | grep -v "grep" | grep -q $NTPD
37 | ; then failure $"ntp shutdown"; else
38 | success $"ntp shutdown"; fi
39 | echo
40 | }
41 | # See how we were called.
42 | case "$1" in
43 | start)
44 | start
45 | ;;
46 | stop)
47 | stop
48 | ;;
49 | restart|reload)
50 | stop
51 | start
52 | ;;
   | *)
   | echo $"Usage: $0 {start|stop|restart}"
   | exit 1
   | esac
   | exit 0

```

```

1 | # chmod 755 /etc/init.d/ntp

```

- Start services:

```

1 | # /etc/init.d/named start
2 | # /etc/init.d/ntp start
3 | # /etc/init.d/samba4 start

```

- Initialize services at boot time:

```

1 | # chkconfig --levels 235 samba4 on
2 | # chkconfig --levels 235 ntp on
3 | # chkconfig --levels 235 named on

```

- Adding iptables rules:

```

1 | # vi /etc/sysconfig/iptables
2 |
3 | -A INPUT -m udp -p udp --dport 53 -m
4 | comment --comment "DNS" -j ACCEPT
5 | -A INPUT -m udp -p udp --dport 123 -m
6 | comment --comment "NTP" -j ACCEPT
7 | -A INPUT -m udp -p udp --dport 135 -m

```

```
8 | comment --comment "RPC UDP" -j ACCEPT
9 | -A INPUT -m udp -p udp --dport 138 -m
10 | comment --comment "NetBIOS Netlogon and
11 | Browsing" -j ACCEPT
12 | -A INPUT -m udp -p udp --dport 389 -m
13 | comment --comment "LDAP UDP" -j ACCEPT
14 | -A INPUT -m state --state NEW -m tcp -p
15 | tcp --dport 88 -m comment --comment
16 | "Kerberos" -j ACCEPT
17 | -A INPUT -m state --state NEW -m tcp -p
    tcp --dport 464 -m comment --comment
    "Kerberos Password Management" -j ACCEPT
    -A INPUT -m state --state NEW -m tcp -p
    tcp --dport 139 -m comment --comment
    "NetBIOS Session" -j ACCEPT
    -A INPUT -m state --state NEW -m tcp -p
    tcp --dport 445 -m comment --comment "SMB
    CIFS" -j ACCEPT
    -A INPUT -m state --state NEW -m tcp -p
    tcp --dport 389 -m comment --comment
    "LDAP TCP" -j ACCEPT
    -A INPUT -m state --state NEW -m tcp -p
    tcp --dport 636 -m comment --comment
    "LDAP SSL" -j ACCEPT
    -A INPUT -m state --state NEW -m tcp -p
    tcp --dport 3268 -m comment --comment
    "LDAP Global Catalog" -j ACCEPT
    -A INPUT -m state --state NEW -m tcp -p
    tcp --dport 3269 -m comment --comment
    "LDAP Global Catalog SSL" -j ACCEPT

# service iptables restart
```



## Sources

<http://wiki.samba.org/index.php/Samba4/HOWTO>

<https://fedoraproject.org/w/index.php?title=Features/Samba4>

– NTP init script and iptables rules edited by Marc (see the comments), Thanks!!



---

## Related

[A bit of Bind \(Part I\)](#)  
December 6, 2011  
In "DNS"

[A bit of Bind \(Part II\)](#)  
December 23, 2011  
In "DNS"

[Configuring Nagios \(Part I\)](#)  
March 30, 2012  
In "GNU/Linux"