THINGS DO MAKE SENSE

MARCH 26, 2016APRIL 18, 2016 JEFF BALES CENTOS, LINUX, SAMBA

Installing Samba 4.4.0 AD DC on CentOS 7.1511

**** You should upgrade to at least 4.4.2 because of the Badlock Bug (http://badlock.org/), released 4-12-2016 ****

Samba 4.4.0 has several improvements, now allows for a demoting a dead server and it allows me to use a real server if I want to, not only a virtual one, but I still prefer a virtual one though.

I will be using this information for the Samba AD DC server:

Samba Server: dc1
IP Address: 192.168.2.100
Netmask: 255.255.255.0
Default Gateway: 192.168.2.1
DNS Domain Name: bales.lan
NetBIOS Domain Name: BALES
DNS Backend: SAMBA_INTERNAL

After Installing CentOS:

I installed updates using terminal:

```
sudo yum update
```

then I rebooted.

Then disabled the firewall and disabled SELinux:

```
sudo service firewalld stop
sudo systemctl disable firewalld
```

```
sudo gedit /etc/sysconfig/selinux

# This file controls the state of SELinux on the system.
# SELINUX= can take one of these three values:
#     enforcing - SELinux security policy is enforced.
#     permissive - SELinux prints warnings instead of enforcing.
#     disabled - No SELinux policy is loaded.
SELINUX=disabled
# SELINUXTYPE= can take one of three two values:
#     targeted - Targeted processes are protected,
#     minimum - Modification of targeted policy. Only selected processes are pr
#     mls - Multi Level Security protection.
SELINUXTYPE=targeted
```

Reboot.

Prerequisite CentOS:

I changed the network:

```
sudo gedit /etc/sysconfig/network-scripts/ifcfg-eno16777736

TYPE=Ethernet
BOOTPROTO=static
IPADDR=192.168.2.100
NETMASK=255.255.255.0
GATEWAY=192.168.2.1
DNS1=192.168.2.100
DNS2=192.168.2.1
DEFROUTE=yes
PEERDNS=yes
PEERROUTES=yes
IPV4_FAILURE_FATAL=no
IPV6INIT=yes
IPV6_AUTOCONF=yes
IPV6_DEFROUTE=yes
IPV6_PEERDNS=yes
IPV6_PEERROUTES=yes
IPV6_FAILURE_FATAL=no
NAME=eno16777736
UUID=b949bf38-7e14-43cd-ace2-0fb532a70427
DEVICE=eno16777736
ONBOOT=yes
```

*** Since I used VMware Workstation 12 for my CentOS it had additional interface called “virbr0” and it was using 192.168.22.8 (why that I don’t know), and it was intefering with making Samba AD DC work. I disabled it by doing this:

```
sudo virsh net-destroy default
sudo virsh net-undefine default
sudo service libvirtd restart
```

Then I changed the /etc/hosts file to match the actual IP of my server (dc1):

```
127.0.0.1   localhost localhost.localdomain localhost4 localhost4.localdomain4
192.168.2.100 dc1.bales.lan dc1
::1         localhost localhost.localdomain localhost6 localhost6.localdomain6
```

Then changed to the hostname to only ‘dc1’:

```
sudo gedit /etc/hostname
```

Rebooted.

I then changed the path directory by adding’:/usr/local/samba/bin:/usr/local/samba/sbin’ a new file called samba-path.sh in the /etc/profile.d/ directory:

```
sudo gedit /etc/profile.d/samba-path.sh

PATH=${PATH}:/usr/local/samba/bin:/usr/local/samba/sbin
```

Then I added the same line to the sudoers file in the ‘Defaults secure_path’ line:

```
sudo gedit /etc/sudoers

.........
#
# Defaults   env_keep += "HOME"

Defaults    secure_path = /sbin:/bin:/usr/sbin:/usr/bin:/usr/local/samba/bin:/u

## Next comes the main part: which users can run what software on
## which machines (the sudoers file can be shared between multiple
## systems).
## Syntax:

.........
```

Then I rebooted again.

After rebooting install the requirements/dependencies for Samba AD DC:

```
sudo yum install perl gcc attr libacl-devel libblkid-devel \
   gnutls-devel readline-devel python-devel gdb pkgconfig \
   krb5-workstation zlib-devel setroubleshoot-server libaio-devel \
   setroubleshoot-plugins policycoreutils-python \
   libsemanage-python perl-ExtUtils-MakeMaker perl-Parse-Yapp \
   perl-Test-Base popt-devel libxml2-devel libattr-devel \
   keyutils-libs-devel cups-devel bind-utils libxslt \
   docbook-style-xsl openldap-devel autoconf python-crypto pam-devel
```

Rebooted.

Installing Samba AD DC:

Download the 'samba 4.4.0' zipped file from http://www.samba.org (http://www.samba.org/) and extract it to your Downloads directory. Using terminal first do a ./configure in the extraction directory:

```
sudo ./configure
```

Then a make:

```
sudo make
```

Then lastly make install:

```
sudo make install
```

Rebooted.

Time to build the Samba AD DC:

```
sudo samba-tool domain provision --use-rfc2307 --interactive
```

```
Realm [BALES.LAN]:
 Domain [BALES]:
 Server Role (dc, member, standalone) [dc]:
 DNS backend (SAMBA_INTERNAL, BIND9_FLATFILE, BIND9_DLZ, NONE) [SAMBA_INTERNAL]
 DNS forwarder IP address (write 'none' to disable forwarding) [192.168.2.100]:
Administrator password:
Retype password:
Looking up IPv4 addresses
Looking up IPv6 addresses
No IPv6 address will be assigned
Setting up share.ldb
Setting up secrets.ldb
Setting up the registry
Setting up the privileges database
Setting up idmap db
Setting up SAM db
Setting up sam.ldb partitions and settings
Setting up sam.ldb rootDSE
Pre-loading the Samba 4 and AD schema
Adding DomainDN: DC=bales,DC=lan
Adding configuration container
Setting up sam.ldb schema
Setting up sam.ldb configuration data
Setting up display specifiers
Modifying display specifiers
Adding users container
Modifying users container
Adding computers container
Modifying computers container
Setting up sam.ldb data
Setting up well known security principals
Setting up sam.ldb users and groups
Setting up self join
Adding DNS accounts
Creating CN=MicrosoftDNS,CN=System,DC=bales,DC=lan
Creating DomainDnsZones and ForestDnsZones partitions
Populating DomainDnsZones and ForestDnsZones partitions
Setting up sam.ldb rootDSE marking as synchronized
Fixing provision GUIDs
A Kerberos configuration suitable for Samba 4 has been generated at /usr/local/
Setting up fake yp server settings
Once the above files are installed, your Samba4 server will be ready to use
Server Role: active directory domain controller
Hostname: dc1
NetBIOS Domain: BALES
DNS Domain: bales.lan
DOMAIN SID: S-1-5-21-3029194575-1187518308-3507572050
```

* Administrator password:

At least 8 characters
Containing at least three of the following five character groups:

- Uppercase characters of European languages (A through Z, with diacritic marks, Greek and Cyrillic characters)
- Lowercase characters of European languages (a through z, sharp-s, with diacritic marks, Greek and Cyrillic characters)
- Base 10 digits (0 through 9)
- Nonalphanumeric characters: ~!@#$%^&*_-+=`|\(){}[]:;"',.?/
- Any Unicode character that is categorized as an alphabetic character but is not uppercase or lowercase. This includes Unicode characters from Asian languages.
  If the password doesn't fulfil the complexity requirements, the provisioning will fail and you will have to start over (remove the generated new "smb.conf" in that case).

Testing your Samba Domain Controller:

First start samba*:

```
sudo samba
```

* Samba does not have init script for samba4.

Testing my Samba AD DC default netlogon and sysvol shares:

```
$ smbclient -L localhost -U%
Domain=[BALES] OS=[Windows 6.1] Server=[Samba 4.4.0]

        Sharename       Type      Comment
        ---------       ----      -------
        netlogon        Disk
        sysvol          Disk
        IPC$            IPC       IPC Service (Samba 4.4.0)
Domain=[BALES] OS=[Windows 6.1] Server=[Samba 4.4.0]

        Server               Comment
        ---------            -------

        Workgroup            Master
        ---------            -------
```

To test that authentication is working, I connected to the netlogon share, using the Domain Administrator account, that was created during provisioning:

```
$ smbclient //localhost/netlogon -UAdministrator -c 'ls'
Enter Administrator's password: *
Domain=[BALES] OS=[Windows 6.1] Server=[Samba 4.4.0]
 .                                   D        0  Sat Mar 27 08:40:00 2016
 ..                                  D        0  Sat Mar 27 08:40:00 2015

               59732092 blocks of size 1024. 52582052 blocks available
```

To test that DNS is working properly, I ran the following commands:

```
$ host -t SRV _ldap._tcp.bales.lan
_ldap._tcp.bales.lan has SRV record 0 100 389 dc1.bales.lan
```

```
$ host -t SRV _kerberos._udp.bales.lan
_kerberos._udp.bales.lan has SRV record 0 100 88 dc1.bales.lan
```

```
$ host -t A dc1.bales.lan
centos.bales.lan has address 192.168.2.100
```

Use “kinit” to obtain a Kerberos ticket:

```
$ kinit administrator@BALES.LAN
Password for administrator@BALES.LAN:
Warning: Your password will expire in 41 days on Sat 07 May 2016 10:13:04 AM PI
```

Note: You must always specify your realm in uppercase letters!

```
$ klist
Ticket cache: KEYRING:persistent:1000:1000
Default principal: administrator@BALES.LAN

Valid starting       Expires              Service principal
11/09/2015 13:32:44  03/29/2016 23:32:44  krbtgt/BALES.LAN@BALES.LAN
        renew until 04/02/2016 13:32:39
```

No error message, you are ready to go! But you do or something is going wrong, see the Samba AD DC Troubleshooting (https://wiki.samba.org/index.php/Samba_AD_DC_Troubleshooting) page.

References:

https://wiki.samba.org/index.php/Samba_AD_DC_HOWTO
(http://askubuntu.com/questions/246343/what-is-the-virbr0-interface-used-for)
http://askubuntu.com/questions/246343/what-is-the-virbr0-interface-used-for
(http://askubuntu.com/questions/246343/what-is-the-virbr0-interface-used-for)

TAGGED ACTIVE DIRECTORY, SAMBA ACTIVE DIRECTORY, SAMBA AD DC

Published by **Jeff Bales**

My name is Jeff Bales and I'm a 53 year-old self-employed "computer guy" with several strokes in 2010 and sort of retired, and I and my husband move here to Pahrump. I write about serious things, silly things, about-nothing things, techie things and other stuff. View all posts by Jeff Bales

CREATE A FREE WEBSITE OR BLOG AT WORDPRESS.COM.