FreeBSD Administration - Support #330

Installing Samba4 On A FreeNAS Jail As A Backup Domain Controller

02/08/2014 03:15 PM - Daniel Curtis

Status:	Closed	**Start date:**	02/08/2014
Priority:	Normal	**Due date:**	
Assignee:	Daniel Curtis	**% Done:**	100%
Category:	Domain Controller	**Estimated time:**	2.00 hours
Target version:	FreeBSD 9	**Spent time:**	8.00 hours

Description

To increase reliability of my Active Directory domain, I have decided to create a backup domain controller in a jail on my FreeNAS server. This guide is document the procedure used to set up the server. Once the jail had been created, I logged into the jail via ssh:

```
ssh root@dc1.example.com
```

Install Samba4

Begin by installing BIND 9.8, samba4, and Heimdal Kerberos via pkg:

```
pkg install bind98 heimdal pylibacl py27-xattr samba4
```

NOTE: I chose to use the BIND 9.8 package instead of the default samba internal DNS server, since that is what I am using on the primary domain controller.

Once the package finishes installing, the following is displayed:

> This port is **STILL** experimental, use it at your own risk.
>
> How to start: http://wiki.samba.org/index.php/Samba4/HOWTO
>
> - Your configuration is: /usr/local/etc/smb4.conf
> - All the relevant databases are under: /var/db/samba4
> - All the logs are under: /var/log/samba4
> - Provisioning script is: /usr/local/bin/samba-tool
>
> You will need to specify location of the 'nsupdate' command in the
> smb4.conf file:
>
> nsupdate command = /usr/local/bin/samba-nsupdate -g

This is important to remember, as the smb4.conf file will be created after joining the domain.

Configure /usr/local/etc/krb5.conf

In order to join to the Active Directory domain, Samba and Kerberos need to be configured. Start by editing /etc/krb5.conf:

```
nano /etc/krb5.conf
```

> [logging]
> default = FILE:/var/log/krb5libs.log
> kdc = FILE:/var/log/krb5kdc.log
> admin_server = FILE:/var/log/kadmind.log
>
> [libdefaults]

default_realm = EXAMPLE.COM
ticket_lifetime = 24h
forwardable = yes

[appdefaults]
pam = {
debug = false
ticket_lifetime = 36000
renew_lifetime = 36000
forwardable = true
krb4_convert = false
}

NOTE: Make sure to replace EXAMPLE.COM with the Active Directory Realm.

At this point, I was able to connect to the primary domain controllers Kerberos realm:

```
kinit administrator
```

I verified successful credentials by running:

```
klist
```

Ticket cache: FILE:/tmp/krb5cc_0
Default principal: administrator@example.com

Valid starting Expires Service principal
11/11/12 17:29:51 11/12/12 03:29:51 krbtgt/example.com@example.com
renew until 11/12/12 17:29:49

Now the machine can be joined to the Active Directory domain.

Joining the existing domain as a DC

Make sure, that your /etc/resolv.conf contains at least one nameserver entry, pointing to a DNS, that can resolve your Samba AD zone(s). Example:
nameserver 192.168.0.1

Run the following provisioning command to join to the domain, and specifying to use the BIND9_DLZ backend:

```
samba-tool domain join EXAMPLE.COM DC -Uadministrator@EXAMPLE.COM --use-ntvfs --realm=EXAMPLE.COM
--dns-backend=BIND9_DLZ
```

NOTE: I needed the --use-ntvfs during the joining, or else an error will prevent the joining.

During the join, you should see a set of debug messages about replicating the domains content, like this:

Partition[CN=Configuration,DC=samba,DC=example,DC=com] objects[1614/1614] linked_values[28/0]

At the end, you will see a message like this:

Joined domain SAMBA (SID S-1-5-21-3565189888-2228146013-2029845409) as a DC

Now you have joined your Samba4 server to your existing domain. This will also create a samba4 configuration file at /usr/local/etc/smb4.conf.

Configure /usr/local/etc/smb4.conf

Edit the /usr/local/etc/smb4.conf file and add the configuration parameter noted above:

```
vi /usr/local/etc/smb4.conf
```

```
[global]
...
nsupdate command = /usr/local/bin/samba-nsupdate -g
...
```

Configure BIND

Add the Dynamically Loadable Zone and Kerberos keytab definitions to the BIND configuration:

```
vi /etc/namedb/named.conf
```

```
options {
...
tkey-gssapi-keytab "/var/db/samba4/private/dns.keytab";
...
}
```

Then add the following at the end of the /etc/namedb/named.conf:

```
include "/var/db/samba4/private/named.conf";
```

Enable the service in /etc/rc.conf

```
vi /etc/rc.conf
```

```
named_enable="YES"
named_chrootdir=""
```

Note: Since the BIND server has been set up in jail, it is already chrooted. The default configuration automatically sets up BIND in a chroot environment, and will cause the named service to fail to start unless the named_chrootdir="" is specified in the /etc/rc.conf.

Start the service

```
service named start
```

```
Starting named.
```

And check to see that it is running

```
service named status
```

```
named is running as pid 13260.
```

Enable and start Samba4 service

Enable the service in /etc/rc.conf

```
vi /etc/rc.conf
```

```
ntpd_enable="YES"
samba4_enable="YES"
```

Then start the services:

```
service ntpd start
service samba4 start
```

Resources

- https://bugs.freenas.org/issues/3776
- https://wiki.samba.org/index.php/Samba4/HOWTO/Join_a_domain_as_a_DC

History

#1 - 02/09/2014 03:27 AM - Daniel Curtis

- Description updated

#2 - 02/09/2014 05:59 PM - Daniel Curtis

- Description updated

- % Done changed from 20 to 50

While trying to join to an existing domain I received the following error:

> raise ProvisioningError("Your filesystem or build does not support posix ACLs, which s3fs requires. Try the mounting the filesystem with the 'acl' option.")

This can be resolved by adding the --use-ntvfs flag in the joining command, like so:

```
samba-tool domain join EXAMPLE.COM DC -Uadministrator@EXAMPLE.COM --use-ntvfs --realm=EXAMPLE.COM --dns-backend=BIND9_DLZ
```

#3 - 02/09/2014 06:51 PM - Daniel Curtis

I encountered a problem while trying to add the backup domain controller to the nslcd service used to connect to the Active Directory. I added the extra address to the /etc/nslcd.conf uri parameter, similar to the following:

```
vi /etc/nslcd.conf
```

> #! LDAP/AD server settings
> uri ldap://192.168.0.20:389 ldap://192.168.100.10:389
> base dc=example,dc=com

And then I restarted the nslcd service:

```
service nslcd restart
```

Then verified I had a Kerberos ticket:

```
klist
```

However, I was getting an error in the syslog:

> Feb 9 18:15:03 host1 nslcd[12627]: [8b4567] <passwd(all)> failed to bind to LDAP server ldap://192.168.100.10:389: Local error: SASL: generic failure: GSSAPI Error: Miscellaneous failure (see text) (Matching credential (ldap/192.168.100.10@168.100.10) ...

I found **the solution by adding a PTR record to the Active Directory DNS for the backup domain controller**. Once the DNS record was added I was able to connect to the backup domain controller and get Active Directory information.

#4 - 02/09/2014 07:32 PM - Daniel Curtis

- Description updated

- % Done changed from 50 to 70

#5 - 02/09/2014 08:35 PM - Daniel Curtis

- Status changed from In Progress to Feedback

- % Done changed from 70 to 90

I have the server currently set up as a domain controller and I was able to test that the replication worked by running the following on the BDC:

```
samba-tool user list
```

A valid user list showed that I had successfully joined to the domain as a domain controller.

#6 - 02/19/2014 11:37 AM - Daniel Curtis

- Status changed from Feedback to Closed

- % Done changed from 90 to 100

#7 - 02/15/2015 08:49 PM - Daniel Curtis

- Project changed from 81 to FreeBSD Administration

- Category set to Domain Controller

- Target version set to FreeBSD 9