Journal of Basic and Applied Engineering Research
Print ISSN: 2350-0077; Online ISSN: 2350-0255; Volume 1, Number 8; October, 2014 pp. 55-59

http://www.krishisanskriti.org/jbaer.html

Migration of Windows Intranet domain to Linux Domain Moving Linux to a Wider World

Prema S.[1], Ethirajan D.[2], Senthil Kumar B.[3]

[1]Engineer, CDAC, Chennai, [2]Senior Engineer, CDAC, Chennai
[3]Engineer, CDAC, Chennai

Abstract: **This paper explores both theoretical and practical options for complete migration of Windows Intranet domain controllers to Linux Domain controllers. It talks about the steps to be followed to setup a Linux domain controller which is kept in sync with the existing Windows domain controller in the intranet. Also it addresses the feature enhancements for establishing policies in a Network Migration.**

1. INTRODUCTION

For many companies in the industry, migrating from Windows to Linux makes sense. The reasons are compelling: greater stability and reliability, lower cost, access to application source code, greater security, and conformity with open standards, according to numerous independent studies and industry experts. As vendors, developers and large-scale implementers look for increasing features in Linux desktop operating system, its high time to look for migrating the intranet domain controllers to Linux server solutions. Samba4 is the full replacement for Windows Active Directory interoperability suite of programs for Linux and Unix.

2. WINDOWS DOMAIN CONTROLLER

Active Directory (AD) is a directory service implemented by Microsoft for Windows domain networks. An AD domain controller authenticates and authorizes all users and computers in a Windows domain type network - assigning and enforcing security policies for all computers and installing or updating software.

For example, when a user logs into a computer that is part of a Windows domain, Active Directory checks the submitted password and determines whether the user is a system administrator or normal user. Active Directory makes use of Lightweight Directory Access Protocol (LDAP) versions 2 and 3, Microsoft's version of Kerberos, and DNS.

3. SAMBA4

Samba4 is the complete rewrite of Samba file server from the Samba team. Samba 4.0 can serve as an Active Directory Domain Controller, provide DNS services, handle Kerberos-based authentication, SMB/CIFS server and administer group policy. The Samba 4.0 Domain Controller can even be managed using the native Windows Active Directory admin tools. Samba4 can be installed and setup as a Additional domain controller along with the existing Windows Domain controller in the intranet.

The support for multiple domain controllers in a domain requires two flavors of replication:

- Directory replication (for the user database)
- File system replication (for the sysvol and netlogon shares)

With Samba4 in BOSS GNU /Linux, both the two Windows protocols for replication are implemented and proven to be working.

4. MIGRATION ARCHITECTURE

Consider an organization authenticates all Windows clients using Windows Active directory domain DOMAIN.NET. The key part of the Identity management service includes

- HR
- E-mail
- Login details and policies
- Organization Structure
- Desktop policies

Joining a Samba4 Domain Controller to Windows DC, gets all the key components from Windows AD and keep the objects in synchronization always.

Samba4 embeds its own Winbind implementation. Winbind is responsible for affecting an unix uid to user, gid to groups. It is also used to list groups of a given user, to translate SID to uid/gid and many other things.

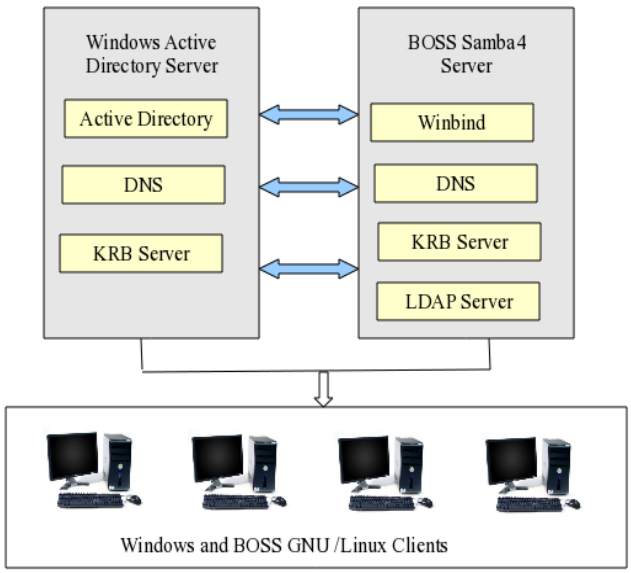

Fig. 1 Windows AD DC and Samba DC

5. GETTING READY FOR MIGRATION

This paper assumes the BOSS Linux Server as the operating system to be installed in the Server and is connected to the Official BOSSLinux repository for package installations.

Samba4 AD services depends on the Hardware capacity of the server for providing the Authentication services. The minimum hardware for a Samba4 server can be determined by the Windows AD server configuration you are currently running. A server equivalent to the current Windows server should be chosen for implementation of Samba4 DC.

5.1 Samba4 Installation

Boot into BOSS 5.0 64 bit version in the server. Before we start, remove any existing Samba 3.x versions in the system.

- apt-get –purge remove samba samba-bin

Once all the previous versions are removed, install the dependency packages for building samba4.

- apt-get build-dep samba4

Download Samba4 from the latest git samba repository.

- git clone git://git.samba.org/samba.git samba

When the samba4 download is over, we are ready to compile and install the binaries. Move to the downloaded path and run

- configure –enable-debugs –prefix=/usr/local/samba –with-ads --with-cups
- make
- make install

The above steps compile and install Samba4 with Active Directory services and Cups services enabled.

5.2 Initial Configuration

Set the DNS entry of the BOSS server pointing to the Windows DNS server. In BOSS server open /etc/resolv.conf file and put the entry for nameserver.

- nano /etc/resolv.conf

Append

- domain DOMAIN.NET
- nameserver DOMAIN.NET

Configure Kerberos server to get authentication from the Windows DC. Open /etc/krb5.conf and keep only below entries.

```
[libdefaults]
dns_lookup_realm = true
dns_lookup_kdc = true
default_realm = DOMAIN.NET
```

Now test that DNS and Kerberos is setup correctly.

```
# kinit administrator
Password: XXXXXXXX
```

klist should give an output similar to this.

```
# klist
Ticket cache: FILE:/tmp/krb5cc_0
Default principal: administrator@domain.net
Valid starting   Expires      Service principal
08/13/13         17:29:51      08/14/13         03:29:51
krbtgt/domain.net@domain.net
 renew until 08/14/13 17:29:49
```

Once all that is setup you can move on to the join domain step.

5.3 Joining Samba4 DC to existing Windows DC

Move to the folder where Samba4 binaries are installed and run the below command.

```
# bin/samba-tool domain join domain.net DC -Uadministrator
–realm=domain.net -W domain.net
```

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. All the User and computer objects along with their GPO are all replicated to the Samba4 DC from the Windows Active Directory DC.

5.4 Checking DNS Records

Before you start samba, you should check, if the new DCs DNS entries are set correctly during joining. This doesn't currently work 100% and have to be done manually in that case.

From the new host, try to resolve its hostname:

- host -t A boss.domain.net.

  If this fails, you have to add the A record by hand. Run on your existing DC:

- samba-tool dns add IP-of-your-DNS-server domain.net BOSS A IP-of-the-DC-you-had-joined -Uadministrator

  Also you should check, if the objectGUID is resolvable to the new hostname. For that, run

- ldbsearch -H /usr/local/samba/private/sam.ldb '(invocationid=*)' --cross-ncs objectguid

  to find out the objectGUID of the new server. The command should give you an output like

- record 1

  dn: CN=NTDS Settings, CN=BOSS, CN=Servers, CN=Default-First-Site-Name, CN=Sites, CN=Configuration, DC=domain, DC=net
  objectGUID: 737506d0-bfe6-40c8-815d-08c3dff7a67f

In this case, 737506d0-bfe6-40c8-815d-08c3dff7a67f is the objectGUID of the new DC, we'll query with the following command:

- host -t CNAME 737506d0-bfe6-40c8-815d-08c3dff7a67f._msdcs.domain.net.

  This should output you the alias (CNAME) of this entry pointing to your new DC name.

  If this record is also missing, you have to add it, too:
  # samba-tool dns add IP-of-your-DNS _msdcs.domain.net 737506d0-bfe6-40c8-815d-08c3dff7a67f CNAME boss.domain.*net*

5.5 Start Samba

Samba DC server can be started from the sbin directory of its installed path.
/usr/local/samba/sbin/samba
Once the Samab4 AD service is started, check out the replication status from the Windows DC.
samba-tool drs showrepl
Default-First-Site-Name\BOSS
DSA Options: 0x00000001
DSA object GUID: 737506d0-bfe6-40c8-815d-08c3dff7a67f
DSA invocationId: eb242434-ca7e-4da7-9b1d-b289ba1922e9
==== INBOUND NEIGHBORS ====
DC=domain, DC=net
Default-First-Site-Name\WINDC via RPC
DSA object GUID: 25e33532-42f2-4082-b9f4-072f9108b565
Last attempt @ Sun Nov 11 18:02:02 2012 CET was successful
0 consecutive failure(s).
Last success @ Sun Nov 11 18:02:02 2012 CET
CN=Configuration, DC=domain, DC=net
Default-First-Site-Name\BOSS via RPC
DSA object GUID: 25e33532-42f2-4082-b9f4-072f9108b565
Last attempt @ Sun Nov 11 18:02:02 2012 CET was successful
0 consecutive failure(s).
Last success @ Sun Nov 11 18:02:02 2012 CET
The above output shows there is a proper replication of all the objects happening between the two Dcs.

5.6 Testing Directory Replication

To check that replication is working correctly between your two domain controllers, try adding a user on the Samba DC using either the Samba command line tools, or the Windows GUI admin tools. Then check that the user shows up within a few seconds on your Windows domain controller.

Similarly, try modifying a user on the Windows domain controller and check that the modifies show up correctly on the Samba server

6. CLIENTS AUTHENTICATION

Now the Samba4 DC is ready, any BOSS or Windows client can be joined and authenticated through the Samba4 DC. There are several solutions available to make BOSS clients to talk with the Samba or Active Directory server. This includes

- Winbind configuration in Clients
- Installing Power Broker open solutions
- Installing CentrifyDC

Out of this Winbind is the easier and light weight protocol that can be implemented and proven in BOSS desktops.

For the described DOMAIN.NET a basic winbind configuration in client is given below.

[global]

workgroup = DOMAIN
security = ads

```
realm = domain.net
password server = boss.domain.com
domain logons = no
template homedir = /home/%D/%U
template shell = /bin/bash
winbind enum groups = yes
winbind enum users = yes
winbind use default domain = yes
domain master = no
local master = no
prefered master = no
os level = 0
idmap config *:backend = tdb
idmap config *:range = 11000-20000
```

With the above winbind configuration, all the user credentials with their policies can be used in BOSS.

7. DOMAIN POLICIES

A domain policy is a high-level container that specifies the company's profile and hierarchy of users in the organization. The policies will be grouped in several levels. In a general Directory domain the policies are defined as

- Password policies
- Hardware policies
- Desktop policies
- OS policies

By default Samba4 supports only Password policies Linux clients that are joined to it. All the other policies can be fulfilled by BOSS Configuration Manager.

BOSS Configuration Manager Architecture

The BOSS Configuration Manager (BCM) works in a server client fashion, wherein all the Linux client machines in the domain should register and get authenticated to the server.

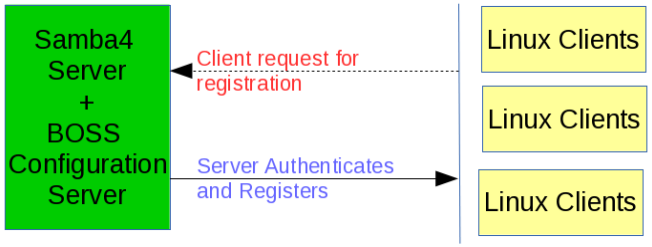

Fig. 2 Server- Client Registration

Each and every client in the domain are identified by a unique name. The unique name is created with a combination of

- Username
- Harddisk id
- Time stamp of the OS installation

The request from the Linux machine with Unique ID is encrypted with the Server SSL key and is sent for Registration over the network. The request is decrypted and is accepted by the server.

7.2 Server – Client Policies

BCM administers Desktop policies, Hardware policies and OS policies in all the connected Linux client machines in the domain. The policies include

Table 1 . BCM Policies

Hardware Policy	Block CD / DVDROM Block USB Block Floppy
OS policy	Services to block Ports to Block Websites to Block Patches to apply Allowed applications to run
Desktop policy	Default Desktop wallpaper Default Screensaver

All the policies are pushed to the client every time the client joins and get authenticates from the server. The Server maintains the policy in a Samba shared file among all the clients.

7.3 Client logs

Apart from pushing the client policies, the BCM provides means to view and retrieve the logs from each of the Linux client machine. The client logs includes

- USB logs
- Web browser logs
- Last login logs
- Su access logs
- Tripwire logs
- Audit logs
- Kernel logs
- Filesystem usage logs

All these logs are filtered and are sent to the BCM server every time after receiving the Policies from the server. The logs can either be only viewed or downloaded completely for the entire month for each of the client machine.

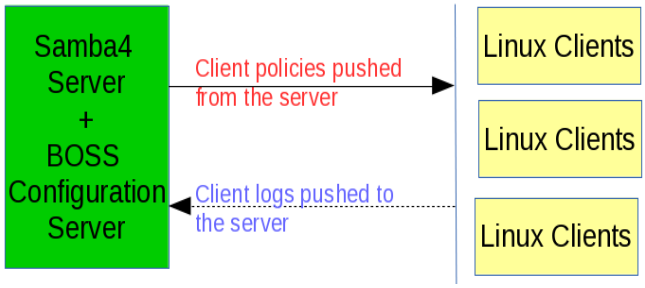

Fig. 3 Policy – Log pushing

All the communication between the server and client are encrypted over SSL and is done through socket connection.

8. SUGGESTED COMPONENTS

In a domain setup there are few other components that need to be addressed on user requirements basis. That includes Mail server integration with the domain and Single-sign-on for all the applications and websites. The mail server integration serves for the Unified mail domain and provides Global Access lists through LDAP in Samba. The Single-sign-on can be achieved and maintained by obtaining the Kerberos tickets for the user session from the server. Both the components can be included successfully in a Samba4 Server.

9. CONCLUSION

Samba4 is successfully deployed and is in function in few of the Client place networks of BOSS project in CDAC. Both the Windows and BOSS Linux clients are getting authenticated from the Samba server. Even though there are few hurdles and issues in migrating the client machines, the basic necessity of Client authentication and authorization is highly managed from Samba sever.

More research and development is involved and going on in Samba for Configuring the Group Policies and better Integration with Mail servers are under development.

10. ACKNOWLEDGEMENTS

This work was supported in part by National Resource Center for Free and Open Source Software - NRCFOSS project by C-DAC – Center for Development of Advanced Computing, Chennai.

REFERENCES

[1] Jelmer R. Vernooij, John H. Terpstra, and Gerald (Jerry) Carter, ”Official Samba HowTo and Reference guide” - May 27 2009

[2] Andrew Abartlet, “Possibilities for Samba 3.0 / Samba4 integration” - 13th Jan 2005

[3] Microsoft guide on Active Directory: http://www.mcmcse.com/microsoft/guides/ad.shtml.

[4] Michael Adam, “Clustering Samba with CTDB, ” samba eXPerience, May 03-07