By Fahd Aziz
Published: 2007-06-25 18:54

Configuring Samba 3.0 To Use The ADSSecurity Mode (CentOS)

This is the first line in the Samba 3.0 release notes:

"Active Directory support. Samba 3.0 is now able to join an ADS (Active Directory Service) realm as a member server and authenticate users using LDAP/Kerberos."

The intent of this article is to show you how to configureyour Linux machine and Samba server to participate in a Windows 2003 ActiveDirectory domain as a Member Server using Kerberos authentication. Thisinvolves using the security = ADS security mode in Samba.

Why would you want to do this? This eliminates the need tocreate separate Samba user accounts on your Linux server so your Windows userscan access the Samba shares. Besides eliminating a lot of administrativeoverhead, without this, you would need to try to keep the password for theSamba user account synched with the password for the user in the AD domain. Ifyou didn't and a Windows user changed his password, he would be prompted for apassword every time he accessed a Samba share.

Probably the main advantage to the security = ADS securitymode is if you are running a Win2003 AD domain in native mode and your securitypolicy prohibits the use of NT-compatible authentication protocols. All of yourworkstations would be Windows 2000 or XP Professional. In this case, Samba was not previously able to act as a Domain Member server in the domain.

If you want to be able to use winbind (discussed in anotherarticle), your Samba server MUST be a domain Member Server.

If you're not familiar with the different AD modes, here's abrief explanation. In mixed mode, all windows clients are able to authenticateto the domain including Win9x, NT4, Win2k, and XP Pro. Samba could also be aMember Server of this domain.

Active Directory in native mode perfectly allows NT4-styleDomain Members. This is contrary to popular belief.

Active Directory in native mode prohibits only the use ofBackup Domain Controllers running MS Windows NT4. Using AD in native mode andrestricting the use of the NT-compatible authentication protocols (i.e., usingKerberos authentication), only Win2k and XP Pro clients can belong to thedomain. If you

have a network with just Win2k and XP Pro clients, this is thepreferred and most secure mode.

Contents

Network Setup

This is the setup on our network:

Linux:

CentOS with Samba 3.0 installed from the RPM package from CentOSCDs.

host/NetBIOS name - *sambaserver* (eth0: *10.0.0.1*)

Win2003:

Windows 2003 Enterprise Server Active Directory (Domain Controller)running SP1

Machine name - *server* (eth0: *10.0.0.1*) (eth1: *192.168.1.1*)

AD domain name - *fahdaziz.com.pk*

Network domain name - *fahdaziz.com.pk*

Running DNS for the entire network (eth0: *10.0.0.0*)

Running DHCP for the entire network (eth0: *10.0.0.0*)

Installing Kerberos

The most crucial thing you need to make this work is to haveKerberos V5 installed on your Linux machine. You will not need to configureyour CentOS machine as a Kerberos server, though.

You can check to see if they are already installed by usingthe *rpm -q* command:

```
rpm -q krb5-libs
```

```
rpm -q krb5-workstation
```

```
rpm -q krb5-server
```

These should return the version numbers, not error messages.

If you don't already have them installed, you can find themon the CentOS CDs. You can install them from the command line using:

```
rpm -ivh <packagename>
```

If your distribution uses RPM packages, try ***www.rpmfind.net***.You can also go to ***http://web.mit.edu/Kerberos/www/index.html*** for the latestrelease of Kerberos.

If you have yum installed on your RPM based distribution,you can execute:

```
yum install krb5-libs
```

```
yum install krb5-workstation
```

```
yum install krb5-server
```

Once you get Kerberos installed on your CentOS machine,there's a few critical things you need to check:
- The time on your Win2003 AD server and your CentOS machine must match. The default Kerberos setting allows for a 5-minute discrepency. I reccomend setting them as close as possible to allow for drift over time. This is ABSOLUTELY CRITICAL! If the clocks don't match, it won't work. This also applies to any other machine in your AD domain you want to authenticate to from your CentOS machine using Kerberos.
- Any user account in the Win2003 AD domain you are going to use for authentication using Kerberos must have had the password changed at least once since it was created. If the password has never been changed since the account was created THIS WON'T WORK!!. On the accounts I used, I just changed the passwords, then changed them right back to their originals.

Installing Samba 3.0

Here's the steps to follow to install Samba 3.0:

1. Remove the old version of Samba from the computer withthis command:

```
rpm -e samba
```

If you installed Samba from the CENTOS CDs, you willprobably have to remove more than one rpm package. You can use the CENTOS GUIpackage manager or execute:

```
rpm -qa | grep samba
```

to list the Samba packages that are installed, thenuninstall them from the command line.

You should uninstall your current version of Samba beforeinstalling Samba 3. When you remove Samba, the rpm command will back up your `smb.conf` file to `smb.conf.rpmsave`. I reccomend you make a backup copy of ityourself though.

If you're not using CentOS, then use the method that isspecific to your Linux distribution to uninstall Samba. If you installed Sambafrom source, see the documentation from ***Samba.org*** to uninstall it.

2. Download and install Samba 3 rpm package for CENTOS.

Once it's downloaded from the Samba.org site, just use:

```
rpm -ivh samba-3.0.0-1.i386.rpm
```

or

```
yum install samba
```

to install it.

If you're not using CentOS, then use the method that isspecific to your Linux distribution to install it. If you are installing Sambafrom source, see the documentation from ***Samba.org*** to install it.

Once you install it, make the `smb.conf.rpmsave` file youractive `smb.conf` file or restore your backup copy of `smb.conf`, then start Samba.Test it to be sure it works as it did before. Your Samba server should work thesame with Samba 3 as it did with Samba 2.2.

Once you've tested Samba 3 to be sure it's working properly,it's CRITICAL that you stop it before you continue with further configuration.If you don't stop Samba, the following attempts to configure it will mostlikely fail.

Configure Kerberos

If you're not familiar with Kerberos, there's a few thingsyou can read to familiarize yourself with it:

The most important thing in configuring Kerberos is the `/etc/krb5.conf` file. There should be an example one in `/etc` you canmodify (that's what I did). If not, then just create one. Here's a copy of mine:

```
[logging]

default = FILE:/var/log/krb5libs.log
```

```
kdc = FILE:/var/log/krb5kdc.log

admin_server = FILE:/var/log/kadmind.log

[libdefaults]

ticket_lifetime = 24000

default_realm = FAHDAZIZ.COM.PK

[realms]

FAHDAZIZ.COM.PK = {

kdc = server.fahdaziz.com.pk

admin_server = server.fahdaziz.com.pk

default_domain = fahdaziz.com.pk

}

[domain_realm]

. fahdaziz.com.pk = FAHDAZIZ.COM.PK

fahdaziz.com.pk = FAHDAZIZ.COM.PK

[kdc]

profile = /var/kerberos/krb5kdc/kdc.conf
```

```
[appdefaults]

pam = {

debug = false

ticket_lifetime = 36000

renew_lifetime = 36000

forwardable = true

krb4_convert = false

}
```

All of the literature I read said the realm name should bein upper case but doesn't have to be. I took their recommendation.

As you can see, I named my realm the same as the AD Domainname. It just so happens that my AD Domain name is the same as my networkdomain name but that's not always the case.

Use your AD DC as the kdc (Key Distribution Center) in your file. Youshould also list it as the admin server. If you have more than one DC in yourAD domain, you can list them as kdc entries.

Once you get your *krb5.conf* file done, you can test it withthe *kinit* command. Execute:

```
kinit username@REALM
```

where username is the name of an account in your AD Domain.It should prompt you for a password. Enter the password for that user in the ADDomain. Note that you must enter the name of the realm in uppercase letters.

If it executes without error, then execute `klist` to see yourKerberos ticket.

Here are the commands I entered:

```
[root@sambaserver home]$ kinit Administrator@FAHDAZIZ.COM.PK

Password for Administrator@FAHDAZIZ.COM.PK:

[root@sambaserver home]$ klist

Ticket cache: FILE:/tmp/krb5cc_500

Default principal: Administrator@FAHDAZIZ.COM.PK

Valid starting Expires Service principal

01/28/07 15:35:40 01/29/07 01:35:40 krbtgt/ FAHDAZIZ.COM.PK @
IVENTSTER.COM.PK
```

```
Kerberos 4 ticket cache: /tmp/tkt500



klist: You have no tickets cached



[root@sambaserver home]$
```

If you get any error messages, make sure that:

- you have no spelling errors in your *krb5.conf* file

- the times are synched on your machines

- the password has been changed at least once on theusername you are using.

Once you get a ticket from the AD DC, test it out by usingKerberos authentication with the *smbclient* command to view the shares on yourWin2k AD DC:

```
smbclient -L /servername -k
```

That should return a list of all the shares on the DC.

Here's how the command worked on my machine:

```
[root@sambaserver home]$ smbclient -L /server -k



Sharename Type Comment
```

```
--------- ---- -------

photos Disk

IPC$ IPC Remote IPC

D$ Disk Default share

rlcowan Disk

NETLOGON Disk Logon server share

Family Disk

ADMIN$ Disk Remote Admin
```

```
SYSVOL Disk Logon server share

Linux Disk

C$ Disk Default share

Server Comment

--------- -------

Workgroup Master

--------- -------

[root@sambaserver home]$
```

After you execute that, you should have another ticket forthe server. You can view it with *klist* like this:

```
[root@sambaserver home]$ klist

Ticket cache: FILE:/tmp/krb5cc_500

Default principal: Administrator@FAHDAZIZ.COM.PK

Valid starting Expires Service principal

09/28/03 15:35:40 09/29/03 01:35:40 krbtgt/ FAHDAZIZ.COM.PK @ FAHDAZIZ.COM.PK

09/28/03 15:42:13 09/29/03 01:35:40 pe500sc$@ FAHDAZIZ.COM.PK

Kerberos 4 ticket cache: /tmp/tkt500

klist: You have no tickets cached
```

```
[root@sambaserver home]$
```

Configure Samba

When you install Samba from the ***Samba.org*** rpm package, itwill also install SWAT. Before you configure Samba, I suggest you fire up SWATand read the document listed on the SWAT home page titled "The Samba HOWTOCollection" It has a section in it that deals with Win2k AD and Kerberos.

You now need to make the changes to your *smb.conf* file toenable Kerberos authentication and so you can join the AD domain. The importantlines in *smb.conf* are:

```
realm = YOUR.REALM

security = ads

password server = <ip address or name of DC>
```

Here's a copy of my *smb.conf* file:

```
[global]

workgroup = fahdaziz

netbios name = sambaserver

server string = Samba Server 3.0

security = ads

realm = FAHDAZIZ.COM.PK

password server = 10.0.0.1
```

```
encrypt passwords = yes

printcap name = /etc/printcap

load printers = yes

printing = cups

log file = /var/log/samba/%m.log

max log size = 0

socket options = TCP_NODELAY SO_RCVBUF=8192 SO_SNDBUF=8192

local master = no

domain master = no

preferred master = no

dns proxy = no

#============================ Share Definitions ==============================

[homes]

comment = Home Directories

browseable = no

writable = yes
```

```
valid users = %S

create mode = 0664

directory mode = 0775

[printers]

comment = All Printers

path = /var/spool/samba

browseable = yes

guest ok = yes

writable = no

printable = yes
```

Once you make the changes to *smb.conf* and before you startSamba, you need to join the AD domain. Before you do so there are two thingsthat you should check:

- If there is a file named */etc/samba/secrets.tdb* eitherdelete, move or rename it. This file would be from your previous connections tothe domain. A new one will be created when you join the domain.

- If there is an existing machine account in your AD domainfor your Samba server, delete it. A new one will be created when you join theAD domain.

Here are the commands I used as root to join the AD domain:

```
kinit Administrator@FAHDAZIZ.COM.PK
```

```
net ads join -Uadministrator%password
```

The first command gets the Kerberos ticket you need toauthenticate to the AD domain. You need to use the username of an account inyour AD domain that has permission to join computers to the domain. The secondcommand joins the domain.

If you're familiar with the command used with Samba 2.2 tojoin a domain, you'll notice the difference. *smbpasswd* is not used any more forthis purpose.

If you successfully join the AD domain, you should receive amessage stating that you successfully joined the Domain. You should also see anew */etc/samba/secrets.tdb* file. There should also be a new machine accountcreated in your Active Directory. If you look at the properties of the machine account, you should see that the OS is listed as Samba 3.0.

Once you've successfully joined the AD domain, start Sambain CentOS using:

```
service smb start
```

or use whatever command you use with your distribution tostart Samba.

One advantage to using this type of authentication is thatyou don't need to create Samba accounts on the Linux server with the *smbpasswd*command. There is no need for the */etc/samba/smbpasswd* file. You Windows usersonly need to be be concerned with one user account.

However, each user that accesses the Samba server will stillneed to have a valid Linux user account on the server that matches the accountin the AD domain. The purpose of this account is to control access to the theLinux file system. The password for that account does not need to match theWin2k AD domain account password. The account doesn't even need to have theability to log in locally to the Linux machine. It does have to exist howeverand it must have the proper permissions to the directories you are sharing outwith Samba for the user to access them. This hasn't changed from Samba 2.2.

To get around the need for for local Linux accounts, youneed to use *winbind*. It'll be interesting to see how that will work inconjuction with an AD domain. But that's the subject of another article.