Samba 4.5 in CentOS 6.8 as

JAMESAREMS

Secondary DC with Microsoft Active Directory 2012R2

Posted by JAMESAREMS *on* OCTOBER 11, 2016

Hi guys ,

This time we are going to discuss about Samba and Windows AD . We can easily integrate Windows AD to Linux using samba packages . Lets start .

Some Notes :

1 . https://bugzilla.samba.org/show_bug.cgi?id=10265

It's necessary to manually lower the domain and forest functional levels on the Windows 2012 server first, via Powershell:

> *Set-ADForestMode -Identity "mydom.local" -ForestMode Windows2008R2Forest*
>
> *Set-ADDomainMode -Identity "mydom.local" -DomainMode Windows2008R2Domain*

2. Need a fresh installed minimal CentOS 6.x OS . Disable SELinux and firewall . Update software packages .

Please check above notes and do as it is . Lets start ,

Primary AD (Microsoft) : 192.168.1.10 / ad.example.com

Secondary DC (CentOS) : 192.168.1.11 / ldap.example.com

Login to Linux server ,

> *# cat /etc/resolv.conf*
>
> *search example.com*
> *nameserver 192.168.1.10*
> *nameserver 192.168.1.11*
>
> *# yum groupinstall "development tools" -y*
>
> *# yum install python-devel libgnutls-dev gnutls-devel libacl1-dev libacl-devel libldap2-dev openldap-devel wget gcc gcc-c++ krb5-server krb5-workstation -y*

> *# wget https://download.samba.org/pub/samba/stable/samba-4.5.0.tar.gz*
>
> *# tar -xvzf samba-4.5.0.tar.gz*

> *# cd samba-4.5.0*
>
> *# ./configure*
>
> *# make*
>
> *# make install*

Now we successfully compiled Samba source package . We need to remove default samba configuration first then remount file system (Some times AD join will popup an ACL error) .

> *# rm -rf /usr/local/samba/etc/smb.conf*
>
> *# mount -o remount,acl,user_xattr /dev/mapper/vg_ldap-lv_root*

Now we are ready to add our Linux machine to Windows AD .

> *# /usr/local/samba/bin/samba-tool domain join example.com DC -Uadministrator –realm=example.com*

Now we successfully added our linux system to Active directory as a Secondary DC . But we need to configure some more settings . Lets check authentication .

Before that check both systems time (NTP) . If its not same authentication will get error .

> *# yum install ntp -y*
>
> *# service ntpd start*
>
> *# chkconfig ntpd on*

Add Our primary DC as NTP server .

> *# vi /etc/ntp.conf*
>
> *server ad.example.com iburst*
>
> *# service ntpd restart*

Now we need to change Kerberos configuration file .

> *# rm -rf /etc/krb5.conf*
>
> *# cp -vr /usr/local/samba/private/krb5.conf /etc/krb5.conf*
>
> *# kinit administrator@EXAMPLE.COM*
>
> *# klist*

For successful AD replication we need to Add A record and CNAME record in Microsoft AD .

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

JAMESAREMS

```
# record 1
dn: CN=NTDS Settings,CN=LDAP,CN=Servers,CN=Default-First-Site-
Name,CN=Sites,CN=Configuration,DC=example,DC=com
objectGUID: 640bcd46-cbc3-4451-8d82-cb37a255cbe1

# record 2
dn: CN=NTDS Settings,CN=AD,CN=Servers,CN=Default-First-Site-
Name,CN=Sites,CN=Configuration,DC=example,DC=com
objectGUID: 89f017ee-dacf-4d51-a19b-fe54da97a79a
```

Copy that ObjectGUID and goto **Microsoft Active directory** .

First create A record for ldap.example.com .

Then goto Forward Lookup Zone > _msdcs.example.com .

Create a CNAME here with our host objectGUID . In my case it is like below ,

640bcd46-cbc3-4451-8d82-cb37a255cbe1 Alias(CNAME) ldap.example.com

Now authentication is working fine .Now we need to start DC replication . Every user created by master or slave need to replicated .

```
# /usr/local/samba/sbin/samba

# /usr/local/samba/bin/samba-tool drs showrepl

Default-First-Site-Name\LDAP
DSA Options: 0x00000001
DSA object GUID: 640bcd46-cbc3-4451-8d82-cb37a255cbe1
DSA invocationId: 4c115875-28b5-4c91-bcf0-66f4d74d935b

==== INBOUND NEIGHBORS ====

DC=DomainDnsZones,DC=example,DC=com
Default-First-Site-Name\AD01 via RPC
DSA object GUID: 89f017ee-dacf-4d51-a19b-fe54da97a79a
Last attempt @ Tue Oct 11 03:13:07 2016 EDT was successful
0 consecutive failure(s).
Last success @ Tue Oct 11 03:13:07 2016 EDT
```

Now we can see that replication is working fine . Lets check now ,

List all AD users.

```
# /usr/local/samba/bin/samba-tool user list
```

JAMESAREMS

Create new user in Active directory and check again . If its showing all is good. Your secondary server is ready to go .

List all member computers .

```
# /usr/local/samba/bin/pdbedit -L -w | grep '\[[WI]'
```

This setup is very useful if you have single windows license and you need Active Directory replica . This is for you .

Enjoy .

Search …

ARCHIVES

- December 2016
- November 2016
- October 2016
- September 2016
- August 2016
- July 2016
- June 2016
- April 2016
- March 2016
- February 2016
- December 2015

TAGS

RECENT POSTS

- ചിന്തയും ആരോഗ്യവും.
- പക എന്ന വിഷം
- Configure WinRM to Use HTTP
- inoERP installation and configuration on CentOS 7
- Samba 4.5 in CentOS 6.8 as Secondary DC with Microsoft Active Directory 2012R2

RECEN COMM