Configuração do domínio (Active Directory) no linux

Leandro Kümmel Tria Mendes

29 de maio de 2013

1 Introdução

Vamos configurar o domínio em uma máquina linux rodando a distribuição FedoraCore 15+, ou seja, válido para versões maiores que a 15.

Todos os comandos referem-se a distribuições da RedHat, ou seja, para Debian, Ubuntu pequenas mudanças, tal como, localização dos arquivos de configuração ocorrerão, para isso consulte http://www.google.com.br

2 Instalações

Para colocar a máquina linux no domínio precisamos instalar alguns pacotes:

- *Kerberos*: Kerberos é o nome de um Protocolo de rede, que permite comunicações individuais seguras e identificadas, em uma rede insegura. O Kerberos previne Eavesdropping e Replay attack, e ainda garante a integridade dos dados. [1]
- *OpenLDAP*: O OpenLDAP é um software livre de código aberto que implementa o protocolo LDAP. Ele é um serviço de diretório baseado no padrão X.500. O OpenLDAP é independente de sistema operativo. Várias distribuições Linux incluem o pacote do OpenLDAP. O software também corre nos sistemas operativos BSD, AIX, HP-UX, Mac OS X, Solaris, Microsoft Windows (2000, XP, 2003, 2008, Vista, win7 e win 8) e z/OS. [2]
- *CUPS*: Um computador rodando o CUPS é um hospedeiro que pode aceitar tarefas de impressão de computadores clientes, processá-los e enviá-los à impressora correta, além disso é possível monitorar impressões, relatar erros de impressões, visualizar relatórios sobre número de páginas impressas, data e horário da mesma.[3]
- *SAMBA*: Samba é utilizado em sistemas operacionais do tipo Unix, que simula um servidor Windows, permitindo que seja feito gerenciamento e compartilhamento de arquivos em uma rede Microsoft. Na versão 3, o Samba não só provê arquivos e serviços de impressão para vários Clientes Windows, como pode também integrar-se com Windows Server Domain, tanto como Primary Domain Controller (PDC) ou como um Domain Member. Pode fazer parte também de um Active Directory Domain. [4]

2.1 Procedimento

2.1.1 Kerberos

$ **sudo yum install krb5-appl-clients.i686 krb5-appl-servers.i686 krb5-pkinit-openssl.i686 krb5-workstation.i686**

2.1.2 OpenLDAP

$ **sudo yum install openldap.i686 openldap-clients.i686 pam_ldap.i686 smbldap-tools.noarch**

[1] http://pt.wikipedia.org/wiki/Kerberos
[2] http://pt.wikipedia.org/wiki/OpenLDAP
[3] http://pt.wikipedia.org/wiki/CUPS
[4] http://pt.wikipedia.org/wiki/Samba_(servidor)

2.1.3 CUPS

CUPS já vem instalado nativo no FedoraCore 15+

2.1.4 SAMBA

$ **sudo yum install samba-winbind.i686 samba-client.i686 samba-common.i686 samba-winbind-clients.i686 samba-winbind-krb5-locator.i686**

3 Configurações

Para todas as configurações mostradas a baixo, utilizamos uma máquina com nome *CPO75*, o domínio é *CPO.UNICAMP.BR* de IP *143.106.193.3*.

3.1 Kerberos

Editar o arquivo localizado em /etc/krb5.conf (adicionar ou alterar as informações existentes)
$ **sudo 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 = CPO.UNICAMP.BR
        dns_lookup_realm = false
        dns_lookup_kdc = false
        ticket_lifetime = 24h
        renew_lifetime = 7d
        forwardable = true
        clockskew = 300
        kdc_timesync = 1
[realms]
        CPO.UNICAMP.BR = {
          kdc = 143.106.193.3
          admin_server = 143.106.193.3
          kdc = 143.106.193.3
        }
[domain_realm]
        .cpo.unicamp.br = CPO.UNICAMP.BR
        cpo.unicamp.br = CPO.UNICAMP.BR
```

Testar a configuração, primeiro teste com uma senha errada, e esta deve dar uma mensagem de erro, depois teste com a senha correta, e nada deve ocorrer.
$ **kinit administrador**

3.2 WinBind e NS

Alterar as linhas do arquivo /etc/nsswitch.conf.
$ **sudo nano /etc/nsswitch.conf**

```
passwd:     files ldap winbind
shadow:     files ldap winbind
group:      files ldap winbind
hosts:      files dns
```

3.3 Samba

Alterar o arquivo localizado em /etc/samba/smb.cfg
$ **sudo nano /etc/samba/smb.cfg**

```
[global]
        netbios name = CPO75
        unix charset = LOCALE
        workgroup = CPO1
        realm = CPO.UNICAMP.BR
        server string = "Samba 3.0.21a w/ ADS Support"
        security = ADS
        log level = 5
        log file = /var/log/samba/LOG.%m
        max log size = 1024
        socket options = TCP_NODELAY SO_RCVBUF=8192 SO_SNDBUF=8
        printcap name = cups
        disable spoolss = Yes
        show add printer wizard = No
        dns proxy = No
        wins server = 143.106.193.3
        ldap ssl = no
        template shell = /bin/bash
        winbind enum users = Yes
        winbind enum groups = Yes
        winbind use default domain = Yes

[temp]
        comment = Diretorio Temporario
        path = /tmp
        read only = No
        cups options = raw
```

Teste a configuração
$ **testparm**

3.4 AuthConfig

Para registrar algumas configurações. $ **sudo authconfig –updateall –enablewinbind –enablewinbindauth –enablewinbindusedefaultdomain**

3.5 Hosts e DNS

Precismos configurar o hostname, e alias, da máquina e seu DNS (windows têm problemas de comunicação com linux)

3.5.1 Hosts

Altere o arquivo localizado em /etc/hosts, alterando o nome da máquina e seu alias. Troque a linha que contém 127.0.0.1 pela apresentada logo abaixo. $ **sudo nano /etc/hosts**

```
127.0.0.1                cpo75.cpo.unicamp.br  cpo75
```

3.5.2 resolv.conf - DNS

Altere o arquivo localizado em /etc/resolv.conf , nele devem conter no minimo as três linhas abaixo, na ordem apresentada.

```
search cpo.unicamp.br
nameserver 143.106.193.1
nameserver 143.106.2.5
```

4 Iniciar serviços

Rode os três comandos a seguir.
$ **smbd -D**
$ **nmdb -D**
$ **winbindd -D**

5 Trabalhando em rede

Se tudo ocorreu bem até agora, faltam poucos passos, porém os mais problemáticos.

5.1 Net ADS join

Digite o comando abaixo.
$ **sudo net ads join -U administrator**
Caso encontre o erro: *Failed to join domain: failed to lookup DC info for domain 'CPO.UNICAMP.BR' over rpc: Logon failure*, prossiga sem medo.

5.2 smbclient

Digite o comando abaixo, pode se utilizar qualquer usuário, não necessáriamente o administrador.
$ **sudo smbclient -U administrador -L 143.106.193.3**
Coloque a senha e o resultado esperado é algo parecido com:

```
Domain=[CPO1] OS=[Windows Server 2008 R2 Enterprise 7601 Service Pack 1] Server
```

Sharename	Type	Comment
acervo_dt	Disk	
ADMIN	Disk	Administracao remota

```
        area_transf     Disk
        arquitetura     Disk
        arquivo_morto   Disk
        BKPPiniweb      Disk
        C$              Disk      Recurso compartilhado padrao
        do              Disk
        dt              Disk
        E$              Disk      Recurso compartilhado padrao
        estagiarios     Disk
        G               Disk
        G$              Disk      Recurso compartilhado padrao
        H$              Disk      Recurso compartilhado padrao
        htdocs          Disk
        informatica     Disk
        IPC$            IPC       IPC remoto
        logs            Disk
        logs2           Disk
        Luciana         Disk
        NETLOGON        Disk      Compartilhamento do servidor de logon
        ngpo            Disk
        planejamento    Disk
        planes          Disk
        print$          Disk      Drivers de impressora
        ProgramData     Disk
        RH              Disk
        S$              Disk      Recurso compartilhado padrao
        scanstate       Disk
        secretaria      Disk
        SQLExpress      Disk
        SYSVOL          Disk      Compartilhamento do servidor de logon
        temp            Disk
        Users           Disk
Connection to 143.106.193.3 failed (Error NT_STATUS_CONNECTION_REFUSED)
NetBIOS over TCP disabled -- no workgroup available
```

É possível utilizar o alias arquiteto, para o endereço 143.106.193.3
$ **sudo smbclient -U administrador -L arquiteto**

6 Montar/Mapear a máquina arquiteto

Primeiro precisamos criar um diretório, que chamaremos de area_transf e monta-lo em /mnt/
$ **sudo mkdir -p /mnt/area_transf**
$ **sudo mount -t cifs -o rw,noperm,user=¡USUARIO¿,password=¡SENHA¿ //arquiteto/area_transf /mnt/area_transf**
Por último, para testar.
$ **sudo ls -l /mnt/area_transf**