Controlador de Domínio para workstations Windows XP, em Servidores FreeBSD com SAMBA e OpenLDAP

Autoria de Danton Dorati
25/11/2007
Última Atualização 01/05/2010

Depois de algum tempo sem contribuir com a comunidade Brasileira de Usuários de FreeBSD (FUG), Danton Dorati publicou mais um artigo que provavelmente será de ótimo proveito para aqueles que precisam de soluções gratuitas às necessidades nos quesitos segurança e praticidade, tanto para restrições/limitações e/ou facilidade de administração/manutenção respectivamente, no que diz respeito usuários Windows e servidores FreeBSD. Trata-se de um Controlador de Domínio (PDC - Primary Domain Controler) para estações de trabalho Windows XP, com SAMBA e OpenLDAP - protocolos smb e ldap - basicamente fazendo o “papel” do nosso já conhecido AD (Active Directory). E alguns outros aplicativos como, por exemplo, o Ldap Account Manager (LAM) para gerenciamento de “contas de usuários”, grupos, máquinas, “políticas de grupos”, domínio sendo ainda um belo “frontend” para facilitar a vida daqueles que tem menos “contato” com o “mundo Shell” e que estejam habituados com gerenciadores que possuam Interface Gráfica.

Além dos benefícios reais que essa união de protocolos permite proporcionar àqueles que precisam e/ou queiram aplicativos Open Source, seria facimo incluir nese conjunto um Servidor Proxy com opção de autenticação de usuários utilizando a mesma conta que faria logon no Windows, assim sincronizando e centralizando tudo em um mesmo banco de dados, recomendo para esse serviço o Squid. Pensando em longo prazo, utilizar o então já instalado LDAP para armazenar as contas de um hipotético Servidor E-mail baseado no Qmail que por acaso, tem um belo artigo aqui mesmo na FUG, mas fazendo referências a nossa conhecida M$. Enfim vamos ao que interessa e chega de “blá blá blá”. Antes de tudo seria interessante que você atualize seu sistema para STABLE e com um KERNEL customizado especificamente ao hardware, e quase que obrigatório (sendo realmente necessário) a atualização do PORTS, ganhando com isso velocidade e segurança contra eventuais “bugs” e incompatibilidades com versões diferentes tanto para o sistema como para os aplicativos usados nesse “howto”. Não vou demonstrar como atualizar ambos, pois seria muito extenso para esse artigo e como poderá ser notado ao longo da leitura do mesmo, então vá por partes. Use esse artigo da FUG bem bolado e bem explicativo (nossa comunidade está de parabéns). E depois sim, com tudo "redondo bote a mão na massa”! Aplicativos usados nesse documento FreeBSD 6.2 – STABLE i386 · cyrus-sasl 2.1.22 · openldap-server 2.3.38 · samba 3.0.25a_1,1 · s 0.9.3 · LDAP-Account-Manager-1.0.4 1. Instalando base inicial do PDC 1.1. Vamos comec irá fazer com que autenticação no SAMBA seja segura # cd /usr/ports/security/cyrus-sasl2 ;; make config ;; make install clean O menu de configuração deverá ficar dessa forma, (des)marque o que for necessário para que fique semelhante e de OK Atualizando as novas bibliotecas # ldconfig 1.2. Próximo a ser instalado será o OpenLDAP # /usr/ports/net/openldap23-server # make config # make OPENLDAP23-SERVER_CONFIGURE_ARGS="--enable-crypt" # make install clean Faça com que todos “menu config” de cada “port” fique ao menos semelhante com as imagens introduzidas nesse artigo, pois assim não haverá riscos de alguma compilação/instalação ocasione erros. 1.3. Agora vamos ao SAMBA # cd /usr/ports/net/samba3 # make config # make SAMBA3_CONFIGURE_ARGS="-with-ldapsam" # make install clean Desça com a flecha até chegar à última opção do menu e de OK 1.5. Último que será compilado na base do sistema é o BIND Para todo controlador de domínio necessário um Servidor DNS, já que estamos usando como, base para reunir todas as contas de nosso PDC, seria interessante fazer com que o BIND fosse "buscar" suas "zones" no OpenLDAP. # cd /usr/ports/dns/bind9-sdb-ldap ;; make install clean E faça o download do arquivo "schema BIND" que irá ser adicionado no "conf" do slapd e mova-o para o diretório padrão de esquemas do Servidor LDAP. # fetch http://bind9-ldap.bayour.com/dnszone-schema.txtou# fetch http://www.venaas.no/ldap/bind-sdb/dnszone-schema.txt
mv dnszone-schema.txt /usr/local/etc/openldap/schema/bind.schema 2. Configurando o OpenLDAP para qu interagir com o SAMBA 2.1. Copie o arquivo de esquema do SAMBA para a basta do OpenLDAP #cp /usr/local/share/examples/samba/LDAP/samba.schema /usr/local/etc/openldap/schema/ Importante: Sempre que for feita alguma atualização nos diretórios que contenham arquivos binários (bin,sbin), ou seja, inclusão e/ou exclusão e se seu “sheel” seja “csh” é necessário que execute o comando “rehash”. # rehash Editando o slapd.conf e o ldap.conf para que fique conforme o desejado para nosso PDC # cd /usr/local/etc/openldap # ldap.conf host 127.0.0.1 base dc= dominio,dc=com,dc=br uri ldap://localhost rootbinddn cn=root,dc=dominio,dc=com,dc=br port 389 SIZELIMIT 12 TIMELIMIT 15DEREF never #slapd.conf include /usr/local/etc/openldap/schema/core.schema include /usr/local/etc/openldap/schema/cosine.schema include /usr/local/etc/openldap/schema/inetorgperson.schema include /usr/local/etc/openldap/schema/nis.schema include /usr/local/etc/openldap/schema/samba.schema include /usr/local/etc/openldap/schema/bind.schema referral ldap://localhost # Load dynamic backend modules: modulepath /usr/local/libexec/openldap moduleload back_bdb moduleload back_ldap pidfile /var/run/openldap/slapd.pid argsfile /var/run/openldap/slapd.args # Banco LDAP database bdb suffix "dc=dominio,dc=com,dc=br" # Definimos a conta administradora como "root" rootdn "cn=root,dc=dominio,dc=com,dc=br" # A senha deve ser gerada com o slappaswd. ##Ex: # slappasswd ## New password: ## Re-enter new password: ## {SSHA}e7C9/YlcGzCsk7gCkzVzhYFNB/4DzcGB rootpw {SSHA}e7C9/YlcGzCsk7gCkzVzhYFNB/4DzcGB # Caminho para a base de dados LDAP directory /var/db/openldap-data password-hash {CRYPT} password-crypt-salt-format "1.8s" # índices para otimizar acesso index objectClass,uidNumber,gidNumber eq index cn,sn,uid,displayName pres,sub,eq index memberUid,mail,givenname eq index sambaSID,sambaPrimaryGroupSID,sambaDomainName eq index default sub # ACLs access to

attrs=userPassword,sambaLMPassword,sambaNTPassword by self write by anonymous auth by * none access t
read Se por acaso existir na base do sistema o OpenLDAP e/ou algum(s) (valido para qualquer outro aplicativo já instalado anterior mente por você mesmo ou sendo alguma dependência) outro(s) arquivo(s) “conf’s” customizado, faça um backup deles e reedite-os para que fiquem semelhantes a este. Realize esse procedimento com todos arquivos de configuração caso exista algum editado anteriormente. Crie um arquivo LDIF que conterá a base de dados inicial do openldap que mais tarde será “populado” de forma completa e necessária para que nossas estações de trabalhem de forma precisa e “pensem” que seu controlador de domínio é um Windows Server 2003. # cd /root # touch base.ldif Substitua domínio pelo nome do Domínio de sua rede. Dica: caso haja algum Servidor DNS atuando na rede interna coloque o mesmo nome da “zona”. Copie fielmente o conteúdo abaixo para o arquivo recém criado dn: dc=dominio,dc=com,dc=br
dc: dominio
objectClass: top
objectClass: domain

dn: ou=People,dc=dominio,dc=com,dc=br
ou: People
objectClass: top
objectClass: organizationalUnit

dn: ou=Group,dc=dominio,dc=com,dc=br
ou: Group
objectClass: top
objectClass: organizationalUnit

dn: ou=Computers,dc=dominio,dc=com,dc=br
ou: Computers
objectClass: top
objectClass: organizationalUnit dn: cn=wheel,ou=Group,dc=dominio,dc=com,dc=br objectClass: posixGroup objectClass: top cn: wheel userPassword: {crypt}* gidNumber: 0 memberUid: root memberUid: NOME-DO-USUÁRIO dn: cn=nogroup,ou=Group,dc=dominio,dc=com,dc=br objectClass: posixGroup objectClass: top cn: nogroup userPassword: {crypt}* gidNumber: 65533 dn: cn=nobody,ou=Group,dc=dominio,dc=com,dc=br objectClass: posixGroup objectClass: top cn: nobody userPassword: {crypt}* gidNumber: 65534 dn: uid=root,ou=People,dc=dominio,dc=com,dc=br uid: root cn: Charlie & objectClass: account objectClass: posixAccount objectClass: top userPassword: {crypt}* loginShell: /bin/csh uidNumber: 0 gidNumber: 0 homeDirectory: /root gecos: Charlie & dn: uid=nobody,ou=People,dc=dominio,dc=com,dc=br uid: nobody cn: Unprivileged user objectClass: account objectClass: posixAccount objectClass: top userPassword: {crypt}* loginShell: /usr/sbin/nologin uidNumber: 65534 gidNumber: 65534 homeDirectory: /nonexistent gecos: Unprivileged user dn: uid=NOME-DO-USUÁRIO,ou=People,dc=dominio,dc=com,dc=br uid: NOME-DO-USUÁRIO cn: Nome do Usuário Completo objectClass: account objectClass: posixAccount objectClass: top userPassword: {crypt}* loginShell: /bin/csh uidNumber: 1001 gidNumber: 0 homeDirectory: /home/NOME-DO-USUÁRIO gecos: Nome do Usuário Completo dn: uid=NOME-DA-MÁQUINA$,ou=Computers,dc=dominio,dc=com,dc=br uid: NOME-DA-MÁQUINA$ cn: Info do PC objectClass: account objectClass: posixAccount objectClass: top userPassword: {crypt}* loginShell: /usr/bin/nologin uidNumber: 200 gidNumber: 200 homeDirectory: noexistent gecos: Info do PC dn: cn=NextFreeUnixId,dc=dominio,dc=com,dc=br
objectClass: inetOrgPerson
objectClass: sambaUnixIdPool
uidNumber: 1000
gidNumber: 1000
cn: NextFreeUnixId
sn: NextFreeUnixId dn: zoneName=dominio.com.br,dc=dominio,dc=com,dc=br
objectClass: top
objectClass: dNSZone
relativeDomainName: dominio.com.br
zoneName: dominio.com.br dn: relativeDomainName=dominio.com.br,zoneName=dominio.com.br,dc=dominio,dc=com,dc=br
objectClass: top
objectClass: dNSZone
relativeDomainName: dominio.com.br
zoneName: dominio.com.br
dNSTTL: 3600
dNSClass: IN
SOARecord: ns1.dominio.com.br. hostmaster.dominio.com.br. 1 10800 3600 604800 86400
NSRecord: ns1.dominio.com.br.
NSRecord: ns2.dominio.com.br.
ARecord: IP-DO-SERVIDOR-PDC
MXRecord: 10 mail.dominio.com.br. dn: relativeDomainName=@,zoneName=dominio.com.br,dc=dominio,dc=com,dc=br

objectClass: top
objectClass: dNSZone
relativeDomainName: @
zoneName: dominio.com.br
dNSTTL: 3600
dNSClass: IN
SOARecord: ns1.dominio.com.br. hostmaster.dominio.com.br. 1 10800 3600 604800 86400
NSRecord: ns1.dominio.com.br.
NSRecord: ns2.dominio.com.br.
ARecord: IP-DO-SERVIDOR-PDC
MXRecord: 10 mail.dominio.com.br. dn: relativeDomainName=ns1,zoneName=dominio.com.br,dc=dominio,dc=com,dc=br
objectClass: top
objectClass: dNSZone
relativeDomainName: ns1
zoneName: dominio.com.br
dNSTTL: 3600
dNSClass: IN
ARecord: IP-DO-SERVIDOR-PDC dn: relativeDomainName=ns2,zoneName=dominio.com.br,dc=dominio,dc=com,dc=br
objectClass: top
objectClass: dNSZone
relativeDomainName: ns2
zoneName: dominio.com.br
dNSTTL: 3600
dNSClass: IN
ARecord: IP-DO-NS2

dn: relativeDomainName=mail,zoneName=dominio.com.br,dc=dominio,dc=com,dc=br
objectClass: top
objectClass: dNSZone
relativeDomainName: mail
zoneName: dominio.com.br
dNSTTL: 3600
dNSClass: IN
ARecord: IP-DO-MX dn: relativeDomainName=NOME-DA-MÁQUINA,zoneName=dominio.com.br,dc=dominio,dc=com,dc=br
objectClass: top
objectClass: dNSZone
relativeDomainName: NOME-DA-MÁQUINA
zoneName: dominio.com.br
dNSTTL: 3600
dNSClass: IN
ARecord: IP-DA-MÁQUINA Obs.: Você têm duas opções para editar o conteúdo acima de modo que fique a seu gosto, um sendo mais demorado e arriscado ou esquecer algo causando erros na introdução da base de dados do OpenLDAP, e um outro mais simples, fácil e seguro de fazer alterações de forma homogênea. Esse nosso grande aliado é o SED. A sintaxe é a seguinte: # sed -i.bak 's/dominio/SEU-DOMÍNIO/g' base.ldif Troque SEU-DOMÍNIO pelo nome que você pretende que as maquinas façam logon. Será gerado um arquivo backup do editado pelo SED “base.ldif.bak”, caso você tenha feito algo errado é só fazer “um racover”. 2.2. Agor “suba” o daemon do OpenLDAP (slapd) para que possa inserir o DB criado acima , já aproveitando o embalo vamos adicionar no rc.conf a sintaxe para que o slapd “arranque” junto com o boot do sistema e mudar o dono no diretório onde fica o PID do OpenLDAP # /usr/local/libexec/slapd -h ldap:/// -4 # echo 'slapd_enable="YES"' >> /etc/rc.conf # echo 'slapd_flags="-h ldap:/// -4"' >> /etc/rc.conf # chown -R ldap:ldap /var/run/openldap # ldapadd -x -D cn=root,dc=dominio,dc=com,dc=br -W -f /root/base.ldif Digite a mesma senha criada ainda a pouco para ser colocada no atributo “rootpw” do arquivo slapd.conf. Se ocorrer conforme o esperado (der tudo certo) a “saída” do comando acima será algo parecido com o que se segue: adding new entry "dc=dominio,dc=com,dc=br "
adding new entry "ou=People,dc=dominio,dc=com,dc=br"
adding new entry "ou=Group,dc=dominio,dc=com,dc=br"
adding new entry "ou=Computers,dc=dominio,dc=com,dc=br" adding new entry
"cn=wheel,ou=Group,dc=dominio,dc=com,dc=br" adding new entry
"cn=nogroup,ou=Group,dc=dominio,dc=com,dc=br" adding new entry
"cn=nobody,ou=Group,dc=dominio,dc=com,dc=br" adding new entry
"uid=root,ou=People,dc=dominio,dc=com,dc=br" adding new entry
"uid=nobody,ou=People,dc=dominio,dc=com,dc=br" adding new entry "uid=NOME-DO-USUÁRIO,ou=People,dc=dominio,dc=com,dc=br" adding new entry "uid=NOME-DA-MÁQUINA$,ou=People,dc=dominio,dc=com,dc=br" adding new entry "cn=NextFreeUnixId,dc=dominio,dc=com,dc=br"

Instalaremos agora o pacote que fará o intermédio entro o sistema e o ldap # cd /usr/ports/net/nss_ldap ;; make install clean Após o termino da compilação/instalação vamos configurar o nss-ldap para que possa fazer pesquisas no DB do OpenLDAP. Edite o arquivo nss_ldap.conf e altere somente as 4 linhas abaixo e o restante mantenha o padrão: # ee /usr/local/etc/nss_ldap.conf host 127.0.0.1 base dc=dominio,dc=com,dc=br binddn cn=root,dc=dominio,dc=com,dc=br bindpw SENHA-NÃO-CRIPTOGRAFADA Faça o backup do arquivo nsswitch.conf e deixe conforme o exemplo. # cp /etc/nsswitch.conf /etc/nsswitch.conf.bak # nsswitch.conf passwd: files ldap compat passwd_compat: nis group: files ldap compat group_compat: nis shadow: file filesshells: files Agora vamos fazer um teste para verificar se o sistema está indo buscar informações realmente de dados do OpenLDAP, se as configurações estiverem corretas, provável que o retorno do comando “# id root” seja algo semelhante a isso: # tail -f /var/log/debug Nov 16 21:46:37 NOME-DO-SERVIDOR slapd[53833]: conn=1225 fd=12 ACCEPT from IP=127.0.0.1:64093 (IP=0.0.0.0:389) Nov 16 21:46:37 NOME-DO-SERVIDOR slapd[53833]: conn=1225 op=0 BIND dn="cn=root,dc=dominio,dc=com,dc=br" method=128 Nov 16 21:46:37 NOME-DO-SERVIDOR slapd[53833]: conn=1225 op=0 BIND dn="cn=root,dc=dominio,dc=com,dc=br" mech=SIMPLE ssf=0 Nov 16 21:46:37 NOME-DO-SERVIDOR slapd[53833]: conn=1225 op=0 RESULT tag=97 err=0 text= Nov 16 21:46:37 NOME-DO-SERVIDOR slapd[53833]: conn=1225 op=1 SRCH base="dc=dominio,dc=com,dc=br" scope=2 deref=0 filter="(&(objectClass=posixGroup))" Nov 16 21:46:37 NOME-DO-SERVIDOR slapd[53833]: conn=1225 op=1 SRCH attr=cn userPassword memberUid uniqueMember gidNumber Nov 16 21:46:37 NOME-DO-SERVIDOR slapd[53833]: conn=1225 op=1 SEARCH RESULT tag=101 err=0 nentries=6 text= Nov 16 21:46:37 NOME-DO-SERVIDOR slapd[53833]: conn=1225 fd=12 closed (connection lost) 3. Configurando o SAMBA para que atue como PDC e interaja com OpenLDAP 3.1. Alterando o arquivo de configuração smb.conf # smb.conf [global] dos chars workgroup = DOMINIO-MAIÚSCULO server string = FreeBSD PDC security = user passdb backend = ldapsam:ldap://127.0.0.1/ passwd program = /usr/bin/passwd %u passwd chat = *New*password* %n\n *Retype*new*password* %n\n*passwd:*all*authentication*tokens*updated*successfully* log file = /var/log/samba/%m.log max log size = 50 socket options = TCP_NODELAY IPTOS_LOWDELAY SO_RCVBUF=8192 SO_SNDBUF=8192 # loa printers = yes # printcap name = cups add user script = /usr/local/sbin/smbldap-useradd -m "%u" delete user script /usr/local/sbin/smbldap-userdel "%u" add group script = /usr/local/sbin/smbldap-groupadd -p "%g" delete group script = /usr/local/sbin/smbldap-groupdel "%g" add user to group script = /usr/local/sbin/smbldap-groupmod -m "%u" "%g" dele user from group script = /usr/local/sbin/smbldap-groupmod -x "%u" "%g" set primary group script = /usr/local/sbin/smbldap-usermod -g "%g" "%u" add machine script = /usr/local/sbin/smbldap-useradd -w "%u" logon scr = %U.bat logon path = domain logons = Yes os level = 100 preferred master = Yes domain master = Ye ldap admin dn = cn=root,dc=dominio,dc=com,dc=br ldap delete dn = Yes ldap group suffix = ou=Group ldap idma = ou=Idmap ldap machine suffix = ou=Computers ldap passwd sync = Yes ldap suffix = dc=dominio,dc=com,dc=b ssl = no ldap user suffix = ou=People idmap backend = ldap:ldap://127.0.0.1 idmap uid = 10000-15000 idma 10000-15000 template shell = /usr/bin/nologin admin users = administrator, root hosts allow = 192.168.1., 127.0.0 printing = cups # print command = lpr -P'%p' %s; rm %s queuepause command = disable '%p' queueresume comm enable '%p' delete veto files = Yes veto files = /*.aif/*.avi/*.cpl/*.mid/*.mov/*.mpa/*.mpe/*.mp3/*.mpeg/*.mpg/*.rar/*.scr/*.vbe/*.vbs/*.wav/*.wma/*.wmv/*.pif/*.bat/*.exe/ [ho mes] comment = Home Directories valid users = %S force user = %U read only = No create mask = 060 = 0775 browseable = No [profiles] path = /home/profiles valid users = %U, "@Domain Admins" force user = = No browseable = No [admin$] comment = Diretorio ROOT path = / valid users = @wheel read only = 0664 directory mask = 0775 [cdrom] comment = Drive CD-ROM path = /cdrom read list = nobody, guest, sys @wheel, @nobody read only = No [netlogon] comment = The domain logon service path = /usr/local/etc/samba/n browseable = No share modes = No [publico] comment = Diretorio publico path = /home/Publico read only = mask = 0777 directory mask = 0777 guest ok = Yes ## Configuração para o SAMBA ser um servidor de impressão, o precisa ## estar instalado e alguns outros módulos para que funcionee corretamente,um artigo ## para ajudar co configuração você econtrará nesse link. #[print$] # comment = Printer Drivers # browseable = yes # guest ok = yes # guest ok = no # read only = yes # write list = root #[printers] # comme path = /var/spool/samba # browseable = no # public = yes # guest ok = yes # writable = no # printable = ye = root Vamos “startar” os daemons do samba e adicionar no rc.conf a configuração para iniciar no momento do boot e configurar o SAMBA para sincrozinar as contas com o OpenLDAP. # smbd –D -s /usr/local/etc/smb.conf # nmbd –D -s /usr/local/etc/smb.conf # winbindd –D -s /usr/local/etc/smb.conf # echo nmbd_enable="YES" >> /etc/rc.conf # echo smbd_enable="YES" >> /etc/rc.conf # echo winbindd_enable="YES" >> /etc/rc.conf # smbpasswd -W SENHA-DO-OPENLDAP# smbpasswd -a root 3.2. Proximo passo é configurar o s tools para terminar de “popular” o OpenLDAP com as configurações padrões de um Controlador de Domínio para que possa interagir com as maquinas “logadas” mesmo. # cd /usr/ports/net/smbldap-tools ;; make install clean Aparecerá uma interrogação como essa: ð Auto-install the 1 optional module(s) from CPAN? [n] s Digite um “S” e a instalação continuará. Basta editar os arquivos de configuração no diretório /usr/local/etc/smbldap-tool: # smbldap.conf #O SID você obtém através do comando “# net getlocalsid dominio” SID="SID" sambaDomain="DOMINIO-MAIÚSCULO" slaveLDAP="127.0.0.1" slavePort="389" masterLDAP="127.0.0.1" masterPort="389" ldapTLS="0" verify="" cafile ="" clientcert="" clientkey="" suffix="dc=dominio,dc=com,dc=br" usersdn="ou=People,${suffix}" computersdn="ou=Computer s,${suffix}" groupsdn="ou=Group,${suffix}" idmapdn="ou=Idmap,${suffix}" sambaUnixIdPooldn="cn=NextFreeUnixId,${suffi x}" scope="sub" hash_encrypt="CRYPT" crypt_salt_format="1%.8s" userLoginShell="/usr/sbin/nologin" userHome="/home /%U" userHomeDirectoryMode="700" userGecos="Ldap User" defaultUserGid="513" defaultComputerGid="515" skeletonDir="/etc/skel" defaultMaxPasswordAge="45" userSmbHom

e="\HOSTNAME-SERVIDOR\%U" userProfile="\HOSTNAME-SERVIDOR\profiles\%U" userHomeDrive="Z:" #userScript="%U.bat" ## Caso possua um servidor de e-mail set o abaixo: #mailDomain="dominio.com.br" with_smbpasswd="1" smbpasswd="/usr/local/bin/smbpasswd" with_slappasswd="0" slappasswd="/usr/local/sbin/slappasswd" shadowLastChange="" # smbldap_bind.conf masterDN="cn=root,dc=dominio,dc=com,dc=br" masterPw=" SENHA-NÃO-CRIPTOGRAFADA" Termine com o comando smbldap-populate # rehash # smbldap-populate Adicionaremos algumas contas no sistema, assim possibilitando fazer todos testes possíveis com o PDC. # smbldap-useradd -w NOME-DA-MAQUINA # smbldap-useradd -m -a NOME-DO-USUARIO # smbldap-passwd NOME-DO-USUARIO 3.3. Inician com suporte a LDAP # cd /etc ;; unlink /etc/namedb# rm /usr/sbin/named ;; rehash# mkdir /etc/namedb ;; cd /etc/namedb# pw group add named -g 110# pw user add named -c "User BIND" -d /noexistent -s /sbin/nologin -u 110 -g 110# fetch ftp.internic.net/domain/named.root# touch named.conf Edite o arquivo named.conf e deixe-o lago parecido com isto: # named.conf options {

```
	directory "/etc/namedb";	listen-on { 192.168.1.1; };
	pid-file "/var/log/named/named.pid";
	version "";
};logging {
	channel "named_log" {
		file "/var/log/named/named.log" versions 3 size 5m;
		print-time yes;
		print-category yes;
		print-severity yes;
	};	  category "default" {
		"named_log";
	};
};

	# Clientes que poderão usar o Servidor DNS
	match-clients {
		192.168.1.0/24;
	};	# Efetua a busca recursiva apenas para clientes internos.
	recursion yes;	# Root Domain.
	zone "." {
		type hint;
		file "named.root";
	};

	# Zona dominio.com.br
	zone "dominio.com.br" {
		type master;
		database "ldap
ldap://localhost/dc=dominio,dc=com,dc=br????!bindname=cn=root%2cdc=dominio%2cdc=com%2cdc=br,!x-
bindpw=SENHA 172800";
	};  # mkdir /var/log/named# chown -R named:named /var/log/named /etc/namedb# chmod 700 /var/log/named
/etc/namedb# chmod -R 600 /etc/namedb/* Basta iniciar o BIND e criar um arquivo para que inicialize no boot do sistema #
cd /etc/namedb ;; named -u named -c named.conf# echo 'named_enable="YES"' >> /etc/rc.conf# cp /etc/rc.d/named
/etc/rc.d/named.bak# touch /etc/rc.d/named ;; chmod 755 /etc/rc.d/named Edite o arquivo /etc/rc.d/named para ficar como
o exemplo abaixo: #!/bin/sh
#
#
# PROVIDE:named
# KEYWORD:shutdown. /etc/rc.subrname="named"
rcvar=`set_rcvar`load_rc_config $name: ${named_enable="NO"}
: ${named_conf="/etc/namedb/named.conf"}
command="/usr/local/sbin/named -c /etc/namedb/named.conf"
command_args="-u named"
pidfile=/var/log/named/named.pid
#required_files=${named_conf}
stop_postcmd=stop_postcmdstop_postcmd()
{
	rm -f ${pidfile}
}run_rc_command "$1" Verifique se o serviço está relmente "rodando", o retorno do comando abaixo será algo como o
que se segue: # sockstat -4l |grep namednamed	named	51389 20 udp4	192.168.1.238:53	*:*
named	named	51389 21 tcp4	192.168.1.238:53	*:* E para finalizar, altere o arquivo que o sistema fará "resoluções" de
nomes: # resolv.conf domain dominio.com.brnameserver IP-DO-SERVIDOR 3.4. Instalando e configurando noss
&amp;ldquo;frontend&amp;rdquo; para administração do PDC Certifique-se, antes de instalar o LAM, que há na base do sistema o
```

apache + php instalados e configurados corretamente. Caso não, use o exemplo de como configura-los a partir deste artigo “pegando” partes dele. # cd /usr/ports/sysutils/ldap-account-manager ;; make install clean Adicione um “alias” no “httpd.conf” do diretório /usr/local/www/lam.E confirme se no arquivo php.ini contém as linhas abaixo: # echo 'Alias /lam/ "/usr/local/www/lam/"' >> /usr/local/etc/apache22/httpd.conf # php.ini register_globals = Off file_uploads = On Editando os arquivos de configuração do LAM. # cd /usr/local/www/lam/config # config.cfg password: COLOCAR-UMA-SENHA-QUALQUER default: lam # lam.conf serverURL: ldap://localhost:389 admins: cn=root,dc=dominio,dc=com,dc=br passwd: COLOCAR-UMA-SENHA-QUALQUER (DO ARQUIVO CONFIG.CFG) treesuffix: dc=dominio,dc=com,dc=br maxlistentries:10000defaultLanguage: pt_BR.utf8:UTF-8:Portugues (Brasil) scriptPath: scriptServer: cachetimeout: 5 # Module settings modules: posixAccount_minUID: 10000 modules: posixAccount_maxUID: 30000 modules: posixAccount_minMachine: 50000 modules: posixAccount_maxMachine: 60000 modules: posixGroup_minGID: 10000 modules: posixGroup_maxGID: 20000 modules: posixGroup_pwdHash: SSHA modules: posixAccount_pwdHash: SSHA activeTypes: user,group,host,smbDomain types: suffix_user: ou=People,dc=dominio,dc=com,dc=br types: attr_user: #uid;#givenName;#sn;#uidNumber;#gidNumber types: modules_user: inetOrgPerson,posixAccount,shadowAccount,sambaSamAccount types: suffix_group: ou=Group,dc=dominio,dc=com,dc=br types: attr_group: #cn;#gidNumber;#memberUID;#description types: modules_group: posixGroup,sambaGroupMapping types: suffix_host: ou=Computers,dc=dominio,dc=com,dc=br types: attr_host: #cn;#description;#uidNumber;#gidNumber types: modules_host: account,posixAccount,sambaSamAccount types: suffix_smbDomain: sambaDomainName=DOMINIO-MAIÚSCULO,dc=dominio,dc=com,dc=br types: attr_smbDomain: sambaDomainName:Domain name;sambaSID:Domain SIDtypes: modules_smbDomain: sambaDomain scriptRights: 755
modules: sambaSamAccount_timeZone: -3
Depois de tudo editado e dentro dos conformes, abra um navegador qualquer e coloque na barra de endereços http://IP-DO-SERVIDOR-PDC/lam/, irá abrir uma tela de login coloque a mesma senha criada anteriormente com o comando slappasswd. Nosso Servidor PDC já está concluído! Agora temos que fazer uma "workstation” ingressar no DOMINIO, siga os passos a baixo que tudo ocorrerá de forma redonda. 4. Configurando uma "maquina" par membro do DOMINO Faça o download do arquivo ".reg" que irá perminitir que sua estação faça parte do domínio recem criado, pois o Windows XP "encherga" o PDC do SAMBA como se fosse um Sistema Operacional Windows antecessor ao Server 2000, e como sempre, a M$ arruma uma forma de bloquear soluções mais baratas ou até mesmo gratuitas, em fim, basta executar o arquivo com um duplo-click e aceitar "dando" OK que tudo se resolverá. Crie um arquivo no "bloco de notas" com a extenção ".reg" e o
conteúdo: [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Netlogon\Parameters]
"DisablePasswordChange"=dword:00000000
"maximumpasswordage"=dword:0000001e
"requiresignorseal"=dword:00000000
"requirestrongkey"=dword:00000000
"sealsecurechannel"=dword:00000001
"signsecurechannel"=dword:00000001
"Update"="no" Execute-o e confirme o pedido de edição do registro, logo após vá ao "Menu Iniciar" do Windows, click em executar e digite "%SystemRoot%\system32\secpol.msc /s". Abrirá o menu de "configuraçõs locais de segurança" extenda o sub-menu "Diretiva de contas" e logo em seguinda faça o mesmo em "Opções de segurança", dentro dessa janela, desabilite as 3 opções abaixo: Membro do domínio: assinar digitalmente dados do canal seguro (quando for possível)Membro do domínio: criptografar digitalmente dados do canal seguro (quando for possível)Membro do domínio: criptografar ou assinar digitalmente os dados de canal seguro (sempre) Depois de realizado todos esses processos, vamos incluir uma estação Windows XP no PDC. 1) Click com o botão direito do mouse no ícone "Meu Computador" e selecione a última opção do menu (Propriedades). 2) Seleciona a aba "Nome do computador" e click no último botão dessa guia (Alterar). 3) Mude o conteúdo do campo que está selecionado para o nome do computador que adicionamos no SAMBA (NOME-DA-MÁQUINA). 4) Logo abaixo click no botão "Mais ..." e adicione o sufixo dominio.com.br e finalize com OK. 5) Ainda na mesma guia mude a opção, "Membro de" de "Grupo de trabalho" para "Domínio" digite em maiúsculo somente o nome do domínio (DOMNIO). 6) Em seguida aparecerá uma janela de login e senha, digite os dados cadastrados com o comando # smbpasswd -a root Se tudo fluir de forma correta logo após o ingresso ao Domínio, aparecerá uma mensagem do tipo "Bem vindo ao domínio DOMÍNIO" e solicitando junto com ela que reinicie o sistema para que possa finalizar o processo executado anteriormente. Agradecimetos: À todos aqueles que tiveram paciência em esperar esse artigo ficar pronto, pois eu já havia prometido para enumeras pessoas, inclusive ao Lippe que deu uma mão com a edição do mesmo. Caso haja algum problema durante a realização das etapas deste documento ou então alguém que não tenha entendido algo e até mesmo terem percebido problemas e falhas durante a leitura, peço que envie um e-mail para urisso@bsd.com.br.