Samba4

da instalação a administração

Sumário

considerações iniciais

O samba4 nesse ambiente foi instalado em um servidor com Debian 7.2, em sua última revisão e pacotes atualizados.

Um adendo importante é sobre o DNS, serviço indispensável ao samba4. Nos repositórios oficiais do Debian, o Bind não é compatível com zonas DLZ, fazendo não iniciar junto com o Samba4, quando integrado a ele.

Outro é o DNS interno do Samba4, que apesar de ser uma opção interessante para pequenos ambientes, não tem os mesmos recursos do BIND. Um recurso desses, de extrema importância em termos de segurança, são o uso de dnssec para zonas, usando chaves criptograficas e integração com o kerberos.

Ainda nesse assunto, a atualização de endereços atribuidos por DHCP pode ser feito pelo DNS do Samba4, porém sem segurança como no BIND

configuração inicial do servidor

Sistema de arquivos

O sistema de arquivos deve suprir a capacidade de trabalhar com arquivos com níveis de permissões baseados em acls. Isso é conseguido com ATTR e ACL no linux.

É necessário que esses recursos estejam instalados no servidor, ou em último caso, em um sistema de arquivos que não suporte o recurso, como o xfs, seja emulado pelo samba4

No /etc/fstab deixe como abaixo.

Device	*mountpoint*	*filesystem*	*options*	*check*	
/dev/sda1	*/*	*ext4*	*defaults*	*0*	*2*
/dev/sda2	*/srv*	*ext4*	*user_xattr,acl,defaults*	*0*	*0*

hostnames, hosts, nsswitch

Mesmo com o DNS funcional, o linux pode em alguns casos ter problemas de resolução de nomes. Isso ocorre não somente com Linux, mas também com Windows, pois ele busca o “DNS local” antes de um servidor DNS. Ele fica no arquivo hosts.

No arquivo /etc/hosts deixe como abaixo

IP address	*FQDN*	*hostname*
192.168.0.1	*domainserver.domain.local*	*domainserver*
192.168.0.2	*memberdomain.domain.local*	*memberdomain*

O nsswitch no Linux pode auxiliar em resolver problemas de resolução de nomes e é usado para mapear usuários e grupos em outras bases.

Nele é possível determinar as bases de consulta de resolução de nomes,

usuários e grupos, por exemplo.

No arquivo /etc/nsswitch.conf deixe como abaixo.

passwd: compat winbind
group: compat winbind
hosts files dns wins

instalação de pre-requisitos

Usando o Debian como base, temos os pre-requisitos que precisam ser instalados

build-essential libacl1-dev libattr1-dev libblkid-dev libgnutls-dev libreadline-dev python-dev python-dnspython gdb pkg-config libpopt-dev libldap2-dev dnsutils libbsd-dev attr krb5-user docbook-xsl libcups2-dev acl libpamg0-dev

compilação do samba4

Usei a última versão do samba4, a 4.1, que extingue as bibliotecas do swat, entre outros recursos, e o integrei ao sistema de arquivos do Linux. Em algumas literaturas isso não é recomendável, já que uma biblioteca do sistema ao ser atualizada pode sobrescrever uma do samba4.

Adotei esse recurso, visto que nos testes essas atualizações não causaram falhas no samba4.

Compilação do samba4 rápida e integrada ao sistema

Para compilar são necessários o sucesso em 3 fases, configuração do aplicativo para se integrar ao Linux, compilação das bibliotecas necessárias e por fim a instalação.

Extraia o conteúdo do arquivo samba4-versao.tar.gz na pasta /usr/src, e execute:

nice -n -20 ./configure --prefix=/usr --localstatedir=/var --infodir=/usr/share/info --mandir=/usr/share/man --sysconfdir=/etc –enable-fhs

nice -n -20 make -j2 && nice -n -20 make install
o nice irá faze-lo compilar com o máximo de prioridade

configuração inicial do samba4

Após a instalação, os comandos do samba4 estarão disponíveis no PATH dos usuários.

Criação do domínio (Provisionamento)

O samba4 possui um comando para a administração do domínio, e provisionamento.

Configuração de domínio com DNS interno, senha do administrador do domínio (administrator), com nível funcional de domínio e floresta como 2008_R2, última suportada pelo samba4.

Samba-tool domain provision --function-level=2008_R2 –server-role=dc –adminpass=senhacomplexa –dns-backend=SAMBA_INTERNAL

--domain=domain --realm=domain.local --use-xattrs=yes --use-rfc2307

Uma forma mais fácil, e intuitiva, é usar o comando abaixo, para o mesmo resultado

samba-tool domain provision –function-level=2008_R2 –use-rfc2307 –use-xattrs=yes --interactive

arquivos de configuração

Os principais arquivos, logo após o provisionamento são:

/etc/krb5.conf

/etc/samba/smb.conf

O krb5.conf pode ser copiado da pasta /var/lib/samba/private/krb5.conf para /etc/krb5.conf. Entretanto, em nossos testes, o arquivo gerado pelo Debian, pelo dpkg não gera erros de autenticação, desde que esteja com domínio e servidores de autenticação devidamente configurados.

O smb.conf é gerado por padrão pelo samba4, e é o principal arquivo de configuração.

Ele é separado em seções, que em geral são:

[global]

seção de configurações do samba4

[netlogon]

compartilhamento com as GPOs e scripts de logon

[sysvol]

compartilhamento padrao do domínio

[compartilhamentos]

cada compartilhamento entre colchete é lido pelo samba4 e são visualizados pelos usuários

[compartilhamentos_ocultos$]

compartilhamentos ocultos, acessíveis apenas pelo seu nome completo, incluindo o $

Arquivo adotado em cliente

/etc/samba/smb.conf

```
# Global parameters
[global]
        comment = Server domain
        bind interfaces only = yes
        interfaces = eth0,lo
        workgroup = domain
        realm = domain.LOCAL
        netbios name = domainSERVER
        server role = active directory domain controller
```

```
        dns forwarder = 192.168.0.1
        idmap_ldb:use rfc2307 = yes
        allow dns updates = nonsecure
        socket options = TCP_NODELAY SO_RCVBUF=8192
        template shell = /bin/sh
# LOG
        log file = /var/log/samba/samba.log
        log level = 3
        max log size = 1024

[netlogon]
        path = /var/lib/samba/sysvol/domain.local/scripts
        read only = No

[sysvol]
        path = /var/lib/samba/sysvol
        read only = No

[drivers$]
        path = /srv/drivers
        read only = no


[lixeira]
        path = /srv/lixeira
        Comment = Lixeira pública
        read only = no
[Restore]
        path = /Restore
        Comment = Restore de arquivos de backup
        read only = no

[Old]
        path = /srv/old
        comment = Compartilhamento antigo
        read only = no

[publico]
        path = /srv/publico
        comment = Compartilhamento Publico
        read only = no

/etc/krb5.conf

[libdefaults]
        default_realm = DOMAIN.LOCAL
        dns_lookup_realm = false
        dns_lookup_kdc = true

[realms]
        DOMAIN.LOCAL = {
                kdc = domainserver.domain.local:88
                admin_server = domainserver.domain.local:749
                default_domain = domain.local
        }
```

[domain_realm]
.domain.local = DOMAIN.LOCAL
domain.local = DOMAIN.LOCAL

Testes iniciais

Os testes iniciais são baseados em testar resolução de dns, mapeamento de usuários e grupos no domínio, e testar compartilhamentos

DNS

Host -t SRV _ldap._tcp.domain.local

host -t SRV _kerberos._udp.domain.local

host -t A domainserver.domain.local

dig domain.local

mapeamento de usuários e grupos

Getent passwd

getent group

testar compartilhamentos

Smbclient -L localhost -U%

smbclient //localhost/netlogon -Uadministrator -c 'ls'

Administração do AD Samba4

A partir desse ponto, pode-se usar um windows XP Pro, windows 7 pro ou windows 8 para tal função.

Recursos extras

auditoria e lixeira

A lixeira não remove os arquivos e sim os move para uma pasta lixeira, dentro do compartilhamento.

A auditoria faz o acompanhamento do que é feito em arquivos e pastas dentro dos compartilhamentos

/etc/samba/smb.conf

[compartilhamento]
#auditoria e lixeira
vfs objects = recycle full_audit
recycle:facility = LOCAL1

```
        recycle:priority = NOTICE
        recycle:maxsize = 0
        recycle:repository = /srv/lixeira/%S/%U
        recycle:directory_mode = 0750
        recycle:subdir_mode = 0750
        recycle:keeptree = Yes
        recycle:touch = True
        recycle:exclude = *.tmp, *.temp, *.log, *.ldb, *.o, *.obj, ~*.*, *.bak
        recycle:exclude_dir = tmp, temp, cache
        recycle:noversions = .doc|.xls|.ppt|*.dcl
        full_audit:facility = LOCAL5
        full_audit:priority = NOTICE
        full_audit:prefix = %S|%u|%I
        full_audit:success = rename rmdir unlink chown
        full_audit:failure = none
```

Para gerar os logs, é necessário configurar o syslog, ou como usado aqui, o rsyslog. Adicione as linhas nos arquivos indicados abaixo:

/etc/rsyslog.conf

local5.notice /var/log/samba/auditoria.log

verificação de status do servidor

Um script, disponibilizado pelo samba4, e que pode ser colocado num terminal permite o monitoramento em tempo real de todo o servidor samba4. Eu o personalizei para que refletisse informações do domínio que desejava. Eu o coloquei em /usr/local/bin.

```
#!/bin/bash
samba4_path="/usr"
netstat=$(which netstat)
lines=$(tput lines)
columns=$(tput cols)


#check terminal dimensions
test $columns -lt 80 -o $lines -lt 24 && {
        echo -e "Error: Can't run $1.\nNeed at least 24 lines and 80 columns on your terminal. Please
resize the window."
        echo "Please press return to continue"
        read
        exit 1
}

#check for netstat
test "x$netstat" == "x" && {
        echo "Error: Can't run $1. Missing netstat on this system."
        echo "Please press return to continue"
        read
        exit 1
}

get_socket_status()
{
        ip=$1
```

```
	test "$2" == "tcp" && {
		prot="-t"
	} || {
		prot="-u"
	}
	port=$3

	$netstat -lpn -4 $prot | grep "samba[ ]*$" | grep $ip | sed 's/:/ /' | awk '{ print $5 }' | grep $port
>/dev/null 2>&1
	test "$?" == "0" && {
		printf "online"
	} || {
		printf "offline"
	}
}

get_status()
{
	share_cons=$($samba4_path/bin/smbstatus -b 2>/dev/null | awk '{ if (p == 1) { print $0 } ; if ($1
~ "^---") { p=1 } }' | wc -l)

	echo "System time     : $(date +"%F %T %Z")"

	test -z "$dnsips" && return

	firstdnsip=$(echo $dnsips | awk '{ print $1 }')

	displaydnsips="$dnsips"
	test "$dnsips" = "0.0.0.0 " && {
		displaydnsips="$dnsips(all)"
	}

	$samba4_path/bin/samba-tool domain info $firstdnsip 2>/dev/null
	echo "Server IPs      : $serverips"
	echo "DNS listens on  : $displaydnsips"
	echo "Smb connections : $share_cons"
	echo ""
	echo "Services"
	echo "--------"
	echo "DNS (tcp)       : $(get_socket_status $firstdnsip tcp 53)"
	echo "DNS (udp)       : $(get_socket_status $firstdnsip udp 53)"
	echo "Kerberos5       : $(get_socket_status $firstdnsip udp 88)"
	echo "LDAP            : $(get_socket_status $firstdnsip udp 389)"
	echo "kpasswd         : $(get_socket_status $firstdnsip udp 464)"
	echo "SMB             : $(get_socket_status $firstdnsip udp 138)"
	echo "NETBIOS NS      : $(get_socket_status $firstdnsip udp 137)"
}

while [ 0 ] ; do
	for s in '|' '/' '-' '\' ; do
	#get sambas ip
	serverips=$(ip addr | awk '{ if ($1 == "inet" ) printf "%s ", $2 }')
	dnsips=$($netstat -nl -4 -t -p | grep samba | awk '{ print $4 }' | grep -e ":53$" | awk -F: '{ printf
"%s ", $1 }')
	status=$(get_status)
```

```
        clear

        echo "Samba 4 Server Status     $s"
        echo "----------------------------"
        echo "$status"

        if [ "x$dnsips" == "x" ] ; then
                echo -e "\n\nWarning: Samba does not listen on dns port."
                sleep 1
        fi

        sleep 1
        done
done
```

Backup e restore do AD Samba4

O backup, assim como o sambastatus, são disponibilizados por um script feito pelo samba4. Também o personalizei, visto que sem paralisar o serviço, percebi em alguns momentos problemas com restore do banco de dados do serviço. Assim também como enviar e-mail e gravar em log o registro de backup realizado. Também está em /usr/local/bin

```
#!/bin/sh

FROMWHERE=/var/lib/samba
FROMWHERE2=/etc/samba
WHERE=/srv/backup_samba
if [ -n "$1" ] && [ "$1" = "-h" -o "$1" = "--usage" ]; then
        echo "samba_backup [provisiondir] [destinationdir]"
        echo "Will backup your provision located in provisiondir to archive stored in destinationdir"
        echo "Default provisiondir: $FROMWHERE"
        echo "Default destinationdir: $WHERE"
        exit 0
fi

[ -n "$1" -a -d "$1" ]&&FROMWHERE=$1
[ -n "$2" -a -d "$2" ]&&WHERE=$2
# Parando o samba4
echo "Parando o samba4..."
/etc/init.d/samba4 stop
sleep 1
DIRS="private sysvol"
#Number of days to keep the backup
DAYS=90
WHEN=`date +%d%m%y`

if [ ! -d $WHERE ]; then
        echo "Missing backup directory $WHERE"
        exit 1
fi

if [ ! -d $FROMWHERE ]; then
```

```
        echo "Missing or wrong provision directory $FROMWHERE"
        exit 1
fi

cd $FROMWHERE
tar cjf ${WHERE}/smbconf_${WHEN}.tar.bz2 ${FROMWHERE2}/smb.conf >/dev/null 2>&1
if [ $? -ne 0 ]; then
echo "Backup do SMB.conf com erro"
fi
for d in $DIRS;do
        relativedirname=`find . -type d -name "$d" -prune`
        n=`echo $d | sed 's/\//_/g'`
        if [ "$d" = "private" ]; then
                find $relativedirname -name "*.ldb.bak" -exec rm {} \;
                for ldb in `find $relativedirname -name "*.ldb"`; do
                        tdbbackup $ldb
                        if [ $? -ne 0 ]; then
                                echo "Error while backuping $ldb"
                                exit 1
                        fi
                done
                tar cjf ${WHERE}/${n}.${WHEN}.tar.bz2  $relativedirname --exclude=*.ldb >/dev/null 2>&1
                if [ $? -ne 0 ]; then
                        echo "Error while archiving ${WHERE}/samba4_${n}.${WHEN}.tar.bz2" >>
/var/log/domain/backup_error.log;
                        exit 1
                fi
                find $relativedirname -name "*.ldb.bak" -exec rm {} \;
        else
                tar cjf ${WHERE}/${n}.${WHEN}.tar.bz2  $relativedirname >/dev/null 2>&1
                if [ $? -ne 0 ]; then
                        echo "Error while archiving ${WHERE}/${n}.${WHEN}.tar.bz2" >>
/var/log/domain/backup_error.log;
tail -5 /var/log/domain/samba-backup.log | /usr/bin/mutt -s "Erro Backup do Samba4 em `date +
%d-%m-%Y`" sysadmin@gmail.com
                        else
                        echo "Backup de Samba4 com sucesso - `date +%c`" >> /var/log/domain/samba-
backup.log
                        echo "`du -h ${WHERE}/*${WHEN}* | cut -d "/" -f 1,4`" >> /var/log/domain/samba-
backup.log
                        echo "--------------------------------------------------------------------------------" >>
/var/log/domain/samba-backup.log
                        echo "iniciando o samba4..."
                        /etc/init.d/samba4 start
sleep 1
tail -5 /var/log/domain/samba-backup.log | /usr/bin/mutt -s "Backup do Samba4 em `date +%d-%m-
%Y`" relatoriodomain@gmail.com
echo "Relatorio enviado por e-mail..."
                        exit 1
                fi
        fi
done

find $WHERE -name "samba4_*bz2" -mtime $DAYS -exec rm  {} \; >/dev/null 2>&1
```

* os endereços de e-mails foram alterados aqui, e devem estar de acordo com

seu ambiente.