Samba 3 Autenticando em um Domínio AD usando Debian Woody/Sarge Como Plataforma

Este documento foi escrito tendo como base um outro anteriormente gerado por Sulamita Garcia (toskinha@noisemakers.org) porém usando como base o Debian Woody/Sarge (o original usava Slackware) .

O Samba 3 nos trouxe várias novidades, uma delas é a capacidade de participar como Membro Nativo (como se fosse uma máquina rodando Windows 2K/XP) de um Domínio AD (Active Directory) .

As possíveis aplicações são muitas, um servidor de impressão por exemplo, ou um "Atached Storage" barato e com pouquíssima necessidade de gerenciamento, ou mesmo uma estação de trabalho rodando Linux como desktop, se integrando (e se infiltrando ;-) ..) em um ambiente Windows !

As necessidades tanto de Hardware quanto de Software são bem modestas, tenho um simples Pentium 233 MMX com 96 MB de RAM e HD de 4 GB servindo duas impressoras Epson Stylus Color 800 para uma rede de 29 máquinas e a performance é excelente e sem qualquer problema ou reclamação dos usuários, que na sua maioria nem sabe q a máquina roda Linux e não Windows !!

Usei o Debian principalmente pela incrível simplicidade de manutenção proporcionada pelo gerenciador de pacotes apt, e ele também é econômico, toda a instalação (incluindo o Cups e o Samba) ocuparam apenas 390 MB, mas além disto o Debian é uma dais mais completas distribuições existentes (talvez a mais completa mesmo !) com mais de 8.000 pacotes testados e prontos p/uso !

Mãos ao teclado:

Siga as instruções de instalação padrão do Debian Woody, e então adicione um mirror do "testing" (Sarge) ao /etc/apt/sources.list (detalhes no Guia Foca Linux) e então, para facilitar as coisas crie o arquivo /etc/apt/apt.conf e coloque os seguintes parâmetros :

APT::Cache-Limit "67108864" ;
APT::Default-Release "stable" ;

O primeiro aumenta o tamanho do cache do apt, prevenindo qualquer problema devido ao acrescimo de toda a árvore de pacotes do Sarge ao Woody, e o segundo faz com que os pacotes do Sarge sejam usados somente quando você especificar isto como parâmetro do apt .

Para se comunicar com o ADS, o Samba precisa do LDAP e do Kerberos. O LDAP por sua vez precisa do BerkeleyDB (na verdade de um DB, mas a maioria utiliza BerkeleyDB), do Cyrus-SASL, e do OpenSSL. Como o objetivo aqui é tratar do Samba, vamos mostrar rapidamente como instalar estes pacotes, Todos eles presentes nos repositórios oficiais do Debian .

Antes de começar, atualize sua lista de pacotes : apt-get update

OpenSSL - Se vc escolheu a instalação mínima do Debian é provável q vc não tenha a liblioteca OpenSSL instalada, então aproveite e instale um shell seguro que lhe permita gerenciar o seu servidor "escravo" remotamente : apt-get -t testing install ssh

O libssl será instalado ao mesmo tempo pois é uma das dependências do ssh .

Repare no detalhe do "-t testing" na linha de comando do apt, é assim que vc "força" a instalação de pacotes do Sarge, apesar do sistema básico continuar sendo um Woody .

BerkeleyDB – Instale a mais recente versão : apt-get -t testing install libdb4

Cyrus-SASL2 – Aquí você não precisa do Cyrus completo, mas apenas as bibliotecas que permitem a autenticação de usuários : apt-get -t testing install libsasl2

OpenLDAP – Como no ítem anterior, você não precisa do serividor OpenLDAP completo, mas apenas das bibliotecas que permitem a autenticação dos clientes baseados em LDAP :
apt-get -t testing install ldap-gateways ldap-utils libldap2

Kerberos – Assim como nos dois ítens anteriores você só precisa das bibliotecas de autenticação para clientes, mais o arquivo de configuração de exemplo vazio :
apt-get -t testing install libkrb53 krb5-user krb5-config

Durante a instalação destes pacotes o sistema de resolução de dependências sempre lhe pedirá uma confirmação sobre estas dependências, sempre diga sim, o apt-dpkg é bastante sólido, confie nele !

O arquivo de configuração do Kerberos foi automaticamente criado em /etc/krb5.conf, edite-o :

```
[realms]
REALM = {
kdc = servidor
}
```

Onde REALM é o seu realm do ADS, em letras maiúsculas.

Teste sua comunicação com o servidor ADS, autenticando algum usuário existente nele:

```
# kinit usuario@REALM.DO.ADS
password:
```

Se não retornar mensagem alguma, está tudo certo. Se ele retornar:

```
kinit(v5): Clock skew too great while getting initial credentials
```

Verifique o horario e/ou fuso horário e marcações de horário de verão. Se for outro erro, ou é erro de senha ou de configuração, revise seu krb5.conf.
Se for o caso adicione um utilitário de sincronização de relógio : apt-get -t testing install ntp-date

O que interessa: SAMBA
Instale todos os módulos do SAMBA que serão necessários de uma só vez :

```
apt-get -t testing install samba smbclient smbfs winbind
```

Depois disto, temos que criar um smb.conf, e acrescentar estas linhas:

```
security = ADS
password server = endereço_do_ADS
realm = REALM.DO.ADS
```

Para o ADS, e estas abaixo para o winbind:

```
idmap uid = 10000-20000
winbind gid = 10000-20000
winbind enum users = yes
winbind enum groups = yes
template homedir = /tmp
template shell = /bin/bash
```

O próximo passo é adicionar a máquina ao Domínio :

```
net ads join -U Administrator (ou a conta de administrador do w2k)
```

Apos, edite o arquivo /etc/nsswitch.conf, e onde ele especifica a autenticação do sistema substitua:

```
passwd: compat
group: compat
```

por

```
passwd: files winbind
shadow: files
group: files winbind
```

Está quase pronto, reinicie o samba e o winbind:

```
# /etc/init.d/winbind restart
# /etc/init.d/samba restart
```

Verifique a comunicação do winbind, com o comando wbinfo -u. Ele deve retornar os usuarios do ADS. O mesmo com o comando wbinfo -g, só que desta vez retornando os grupos. Se tudo ocorreu bem, com o comando getent passwd deve mostrar os usuarios do sistema seguidos dos usuarios do ADS. Se tudo ocorreu bem até aqui, ótimo, seu samba estará funcionando autenticando os usuários no ADS. Se não funcionou, teste cada um dos passos, principalmente a configuração do kerberos, que é a grande peça de encaixe de tudo.

Fábio Rabelo de Deus
fabior@ajato.com.br