

A próxima versão do servidor universal

Samba do futuro

Em todas as versões do *Samba*, o objetivo é o mesmo: compartilhar recursos do Windows® com sistemas operacionais Unix como o Linux, e compartilhar recursos do Linux com sistemas Windows [1]. Um fator de dificuldade para os desenvolvedores é que o suporte a sistemas Microsoft seja um alvo móvel: Redmond não é exatamente renomada por sua disposição de publicar especificações, e a gigante do software continua estendendo seus protocolos SMB/CIFS a cada versão do Windows.

Os desenvolvedores de código aberto tentam acompanhar as mudanças usando ferramentas como o *Ethereal* para rastrear conexões. Isso costumava funcionar no passado, mas a Microsoft dificultou a situação com o Windows 2000 ao introduzir o sistema de diretórios baseado em objetos chamado *Active Directory Service (ADS)*, [2].

Entretanto, nesse caso a Microsoft buscou padrões estabelecidos, e seus desenvolvedores colocaram um banco de dados de usuários LDAP num mecanismo de autenticação *Kerberos* 5 e optaram pela resolução de nomes baseada em DNS. O fato de que a Microsoft aderiu a padrões verdadeiros abre as portas para o Linux apresentar um alto grau de interoperabilidade, graças às implementações livres como o *OpenLDAP*

e as versões do *Kerberos* com licenças MIT e Heimdal.

Um objetivo principal do Samba 4 é prover um servidor de diretório Samba que consiga interoperar com o *Microsoft Active Directory*, e uma versão bastante preliminar dessa funcionalidade foi liberada no final de janeiro. A equipe do Samba preferiu uma abordagem radical, reimplementando diversas rotinas com o objetivo de tornar o Samba 4 livre de antigas gambiarras que atrapalhavam as versões anteriores. Como consequência, muitas opções das quais o Samba 3 depende foram retiradas.

Kerberos, OpenLDAP e LDB

O Samba 3 deu aos administradores de rede a opção de instalar uma máquina Linux como servidor de domínio num domínio Windows 2000/2003. Do ponto de vista técnico, o servidor usa tíquetes *Kerberos* com fins de autenticação. Baseado nesse design, tanto servidores quanto clientes (usando ferramentas como *smb-mount*) trocam tíquetes, implementando assim operações que requerem somente autenticação uma única vez (*single-sign-on*) entre o Linux e o Windows dentro do domínio. O uso do Samba 3 como

Uma versão de demonstração de novas tecnologias do Samba 4 foi apresentada no final de janeiro. Mostramos aqui as novidades dessa suíte de serviços de arquivos e impressoras.
por Markus Klimke

controlador primário de domínio (*PDC*, ou *Primary Domain Controller*) ou controlador reserva de domínio (*BDC*, ou *Backup Domain Controller*) ficava restrito à autenticação no estilo do Windows NT, com o *Kerberos* adicionado.

Agora que o Samba 4 implementa sua própria funcionalidade *Kerberos*, o

Samba4WINS

O serviço de nomes de Internet do *Windows (WINS)* é uma volta à época do *NT 4*. Dito isto, mais e mais sistemas *Windows* recentes utilizam o protocolo *WINS* para resolver nomes *NetBIOS*. Quando mapeiam um compartilhamento, o nome *NetBIOS* pode ser usado após a primeira contrabarra ou primeiras contrabarras. O Samba já funciona com *NetBIOS* há algum tempo, pois é isso que permite a interoperabilidade entre os servidores. O Samba 4 não mudará isso de forma profunda.

O problema é que servidores *WINS* que utilizam Samba não suportam replicação. Isso não deixa alternativa aos administradores senão gastar dinheiro rodando servidores *WINS* *Windows*. O projeto de cooperação *Samba4WINS* [3] visa a mudar esse quadro. As empresas envolvidas são *Sernet*, *Computacenter* e *Fujitsu Siemens Computers*, além da *Linux Solutions Group e.V.* O *Samba4WINS* será inteiramente integrado ao Samba 4. A funcionalidade pode ser incluída no Samba versão 3.0.21 ou mais recente e executada como um processo independente.



Figura 1 A ferramenta *provision* inicializa o banco de dados do Samba. É possível usar o *Swat* para o mesmo fim.

Samba pode substituir um controlador de domínio moderníssimo no estilo Microsoft (veja abaixo). A implementação do Kerberos usa a variante Heimdal, e naturalmente o desenvolvedor do *Heimdal Love Astrand* teve um papel importantíssimo na equipe de desenvolvimento. No futuro, será possível usar bibliotecas Kerberos externas.

Uma coisa que o Samba 3 nunca conseguiu fazer é a sincronização de bancos de dados de usuários com seus próprios bancos de dados Samba (leia o quadro **Samba4WINS** para mais detalhes). Já que o OpenLDAP consegue replicar seu banco de dados em outros servidores do mesmo tipo, os desenvolvedores do Samba 3 simplesmente esqueceram esse assunto. Entretanto, configurar um servidor OpenLDAP não é nada trivial. A equipe do Samba 4, liderada por Andrew Tridgell, se utilizou de toda essa tecnologia disponível e implementou seu próprio *back-end* LDAP conhecido como *LDB*.

Outro motivo importante para o Samba implementar sua própria solução LDAP é a replicação livre de problemas. Por exemplo, os desenvolvedores queriam migrar mudanças através das máquinas envolvidas para eliminar qualquer risco de replicação inconsistente. Parece bastante que o Samba 4 ainda manterá a capacidade de se ligar ao OpenLDAP, principalmente para suportar ambientes já estabelecidos com servidores Samba 3.

CIFS, NTFS e ACLs Posix

Nunca foi o objetivo do Samba restringir o suporte a ambientes heterogêneos; em vez disso, o Samba sempre teve um papel importante no domínio NFS, suportando o intercâmbio de dados entre sistemas Unix e Linux — chegando ao ponto de competir com o NFS 4, que ainda não está totalmente desenvolvido. Isso fica evidente nos módulos de kernel

relacionados ao CIFS, cujo trabalho de desenvolvimento aumenta a cada versão. Peguemos, por exemplo, as propriedades experimentais do CIFS, que suportam o Kerberos desde a versão 2.6.16. Isso foi uma grande desvantagem em comparação ao SMB do Windows, que permitia aos usuários montar compartilhamentos usando *single-sign-on* com a opção `-o krb`.

No território do gerenciamento de acesso, o Samba já é capaz de mapear *ACLs Posix* em *ACLs NTFS* e vice-versa há algum tempo. Novamente, a versão 4 usa uma abordagem diferente e, em vez de armazenar *ACLs NT* no sistema de arquivos Posix, introduz um sistema de arquivos virtual conhecido como *NTVFS*, que guarda os atributos NTFS como eles estiverem. Ele é até mesmo capaz de emular *ACLs* em *streams* de dados NTFS. *Streams* de dados alternados (*ADS*, ou *Alternate Data Streams*) são uma função do sistema de arquivos NTFS, que permite que os usuários guardem dados de um arquivo de forma alternada e invisível. Políticas de grupo são outro tópico importante da discussão; no momento da escrita deste artigo, não havia certeza sobre como o Samba 4 lidará com eles.



Figura 2 Adicionando um servidor Windows 2003 como um servidor membro de um domínio Samba 4.

Teste de um PDC

Após descompactar o código-fonte do Samba 4.0.0tp1, disponível em [\[4\]](#), procure o arquivo *howto.txt* na árvore do projeto; o arquivo tem algumas dicas interessantes de operação. Após terminar a compilação, você primeiro precisa prover o banco de dados. A ferramenta *provision* se encarrega disso, criando o banco de dados LDAP, o registro, e entradas pré-definidas para acesso ao LDB

Exemplo 1: Saída do testparm

```
# Global parameters
[global]
server role = pdc
workgroup = DOMINIOTESTE
realm = DOMINIOTESTE.ORG
netbios name = LINUX
log level = 2
registry:hkey_users = hku.ldb
registry:hkey_local_machine = hklm.ldb
comment =
path =
ntvfs handler = unixuid, default
read only = Yes
hosts allow =
hosts deny =
max connections = -1
strict sync = No
case insensitive filesystem = No
max print jobs = 1000
printable = No
printer name =
map system = No
map hidden = No
map archive = Yes
browseable = Yes
csc policy = manual
strict locking = Yes
copy =
include =
available = Yes
volume =
fstype = NTFS
msdfs root = No

[dados]
path = /export/dados
read only = No
hosts allow =
hosts deny =

[IPC$]
comment = Servico IPC (Samba 4.0.0tp1)
path = /tmp
ntvfs handler = default
hosts allow =
hosts deny =
browseable = No
fstype = IPC

[ADMIN$]
comment = Servico de DISCO (Samba 4.0.0tp1)
path = /tmp
hosts allow =
hosts deny =
browseable = No
fstype = DISK
```



Figura 3 O Swat permite que você configure um usuário codificado por LDIF; as ferramentas de console oferecem a mesma possibilidade.

e ao servidor DNS dos serviços Kerberos (veja a [figura 1](#)). Ainda será necessário adicionar entradas manualmente à zona para o servidor DNS. O equivalente do Windows à ferramenta *provision* é conhecido como *deprovision*.

O *provision* criará também um *smb.conf* mínimo. Se você passar o prefixo */usr* com o script *configure*, encontrará o arquivo de configuração em */usr/lib* ao final. Para um maior controle, você pode mudar o *daemon* Samba para o modo interativo com o comando *smbd -i -M single*, o que jogará as mensagens na saída padrão. O Samba 4 suporta três modos de operação: ele pode rodar como um único processo, usando *threads*, ou na variante multiprocessado. Assim que o *daemon* estiver rodando e você tiver configurado um compartilhamento de teste, o *testparm* deve gerar uma saída semelhante à do [exemplo 1](#).

De acordo com a equipe do Samba, a versão 4.0.0tp1 é capaz de substituir um PDC. Depois de adicionar as entradas do DNS, nada o impede de adicionar uma máquina Windows ao domínio Samba. Em nosso laboratório, adicionamos um servidor Windows 2003 como servidor membro. Depois de especificarmos o domínio e dizermos que queríamos que a máquina entrasse no domínio, o Windows 2003 pareceu bastante confortável (veja a [figura 2](#)).

Swat revisitado

O gerenciamento de sistemas foi retrabalhado e consideravelmente estendido. Depois de adicionar novas capacidades como Kerberos e LDAP, a equipe do Samba agora deu passos para tornar a

vida mais fácil para o administrador. A ferramenta, bastante conhecida, mas pouco utilizada *Swat* renasceu na versão 4: a interface web agora é parte da suíte Samba. Assim que o *daemon* Samba é iniciado, um servidor embutido compacto *Appweb* [5] fornece a plataforma para o Swat. Isso elimina a necessidade de configurar o Swat, em contraste com as versões anteriores; já é possível navegar pela ferramenta com o seu navegador assim que o *daemon* é iniciado.

O Swat ainda não tem algumas características necessárias para ser considerado

uma interface completa de administração. Mas ele definitivamente consegue mostrar o que o Samba 4 pode fazer no papel de PDC. O usuário padrão é *Administrator*, que deve fazer login usando um cliente Windows. Mas o Swat oferece a possibilidade de adicionar outros usuários.

Como uma alternativa, você pode tentar usar uma das várias novas ferramentas de linha de comando: a que você precisa aqui é a *ldbadd*. Note que o *ldbadd* necessita de um usuário codificado por LDIF. Como o Swat não é capaz de processar isso, a [figura 3](#) mostra como adicionar um usuário ao domínio. Quando um usuário faz seu primeiro login, as configurações do registro do Samba pedem a mudança da senha. O Swat não suporta políticas de senha atualmente.

Supondo que o login esteja funcionando, as credenciais do usuário agora estão guardadas de forma segura no banco de dados LDB do Samba. Se você quiser verificar ou mudar as entradas do banco de dados, pode rodar uma ferramenta de console como o *ldbedit* ou o *ldbsearch*. O primeiro abre o banco de dados no seu editor preferido, onde você pode procurar a entrada do usuário e modificá-la se quiser. A [figura 4](#) demonstra como usar o *ldbsearch*.

O Samba 3 oferecia a possibilidade altamente útil de aceitar um domínio migrado de um servidor Windows NT, e o Samba 4 naturalmente também faz isso.

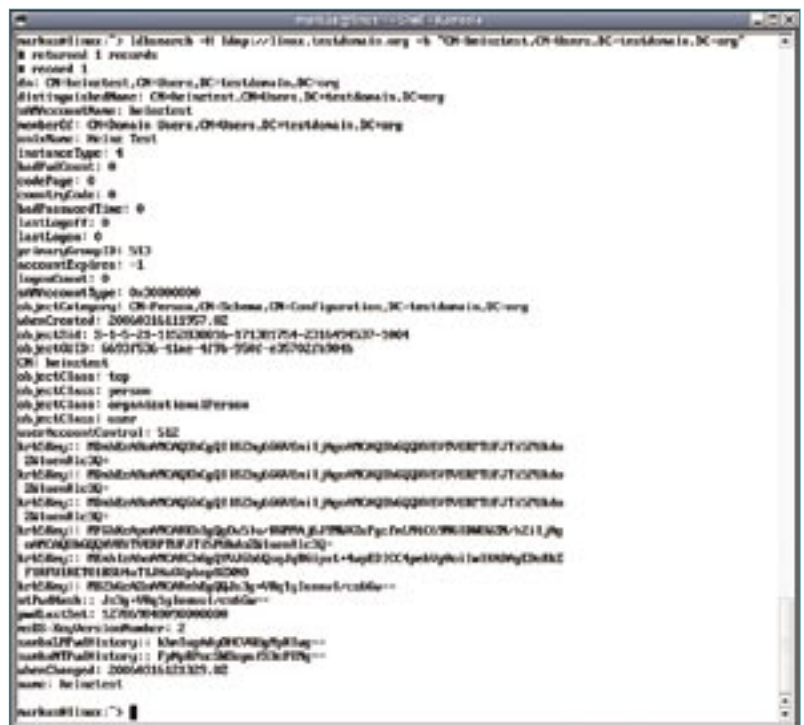


Figura 4 A ferramenta de console do Samba, *ldbsearch*, procurando um usuário.

Os administradores também podem migrar domínios do Samba 3 para o Samba 4 pelo Swat. Este modo “vampiro” não é mais restrito ao Windows NT; agora funciona também com o Windows 2000/2003 Server. Na **figura 5** é possível ver como migramos um domínio do Windows 2003. Só para ter certeza de que o arquivo de log não estava otimista demais, a **figura 6** mostra nossa busca de um usuário no banco de dados LDB do Samba. Nós só queríamos saber se o novo usuário tinha conseguido entrar no novo domínio *win*, e a resposta foi positiva.

Configuração

Editar arquivos de configuração é um método comprovadamente eficiente de sintonia fina. No Samba, o número de arquivos de configuração aumentou sensivelmente. Da mesma forma, algumas opções do Samba 3 foram descartadas. Ainda não está claro quais dessas opções serão retiradas, já que muitas delas ainda permanecem lá para contornar problemas em operações no modo de interoperabilidade.

Novas palavras-chave descrevem o estado e o comportamento do KDC — *kpasswd port* ou *krb5 port*, por exemplo. A opção *paranoid server security* determina um nível de segurança, enquanto *ntvfs handler* especifica como a camada NTVFS deve se comportar. O padrão aqui é *ntvfs handler = unixuid*, que sincroniza as operações de arquivos com o sistema de arquivos Posix abaixo.

A opção *ntvfs handler = cifs* permite que você rode um servidor Samba como uma *gateway* CIFS, que encaminha pedi-

dos de arquivos para outro servidor CIFS. Se o gateway for um servidor membro de domínio, ele pode encaminhar tíquetes de serviços e usuários:

```
[extdata]
ntvfs handler = cifs
cifs:server = nextserver
cifs:share = shared
```

Não existem muitos back-ends para o NTVFS atualmente. Além das opções detalhadas acima, o código-fonte tem a opção *simple*, a qual faz as operações sobre arquivos serem operadas com privilégios de superusuário, tornando-a inútil. Se você precisar de mais informações sobre as opções do *samba.conf*, veja o arquivo *source/param/loadparm.c* no código-fonte.

Independência

De uma forma geral, parece que o Samba 4 finalmente se livrará de suas amarras do passado. Além de LDAP e Kerberos, o software agora consegue lidar com ACLs além do Posix, e tem sua própria emulação de servidor Active Directory. O Samba4WINS fornece serviços de replicação a servidores WINS. Há três modelos para maior escalabilidade: processo único, múltiplos processos como no Samba 3, e uma variante com threads.

Mas atenção: essa demonstração de tecnologia apresentada aqui tem o objetivo de servir como plataforma para a revisão de novas tecnologias. Ela não tem todas as características que esperaríamos em operações de produção. Por exemplo, o



Figura 6 Só para verificar se a migração funcionou direito, nós rodamos o *ldbsearch* para procurar um usuário.

suporte a impressão ainda está faltando. Os desenvolvedores não sugerem que se instale o Samba 4 em ambientes de produção até que eles tenham terminado seu trabalho. Um comunicado público indica que isso não acontecerá antes do fim do ano. A sugestão de alguns desenvolvedores é procurar implementações de novas características (ou seja, *backports*) da versão 4 na versão 3.

A versão 4 não é a única fonte de ocupação dos desenvolvedores do Samba; existe ainda a pequena questão da versão não documentada do Windows Vista SMB 2, que foi completamente reescrita. Se os casos de monopólio na UE contra a Microsoft não tiverem êxito em forçar a empresa a publicar interfaces, a equipe do Samba pretende utilizar novamente sua antiga prática de monitorar transferências de arquivos com o Ethernet. ■

Mais Informações

- [1] Samba: <http://samba.org>
- [2] Active Directory: <http://www.microsoft.com/technet/prodtechnol/windows2000serv/technologies/activedirectory/default.msp>
- [3] Samba4WINS: <http://EnterpriseSamba.org/index.php?id=88>
- [4] Samba 4.0.0tp1: <http://devel.samba.org/samba/ftp/samba4/>
- [5] Appweb Embedded Webserver: <http://www.appwebserver.org>

O autor

Markus Klimke trabalha para o Instituto de Modelagem e Cálculos da Universidade Técnica de Hamburgo-Harburg.



Figura 5 O protocolo Swat seguindo a migração de um domínio do Windows 2003.