NFSv4: Um Padrão Aberto e Sua Relação Com o Software Livre

Renato M. Otranto Jr. , Joaquim Quinteiro Uchôa

Curso de Pós-Graduação *Lato Sensu* em Administração em Redes Linux
Depto. Ciência da Computação - Universidade Federal de Lavras
Caixa Postal 3037 – 37.200-000 – Lavras – MG – Brazil

renato@otrantojr.eng.br,joukim@ginux.ufla.br

Resumo. *Network File System (NFS) é um tradicional sistema de arquivos distribuídos em ambientes Unix, desenvolvido originalmente pela Sun Microsystems. Suas primeiras versões tratavam-se de um protocolo proprietário, mas um acordo entre esta empresa e a Internet Society, permitiu que o controle no desevolvimento do protocolo fosse transferido para uma comunidade internacional e aberta de projetistas e pesquisadores interessados no assunto. Este trabalho visa apresentar algumas das principais características do protocolo, bem como explorar a relação entre a abertura do protocolo e o modelo de desenvolvimento do software livre.*

1. Introdução

Network File System (NFS) é um sistema de arquivos distribuídos desenvolvido originalmente pela Sun Microsystems para compartilhamento de arquivos de forma transparente aos usuários. A primeira versão desse protocolo tratava-se de um protótipo interno da empresa. A versão 2 foi definida pela RFC 1094 (SUN MICROSYSTEMS INC., 1989), mas, apesar de já ser amplamente utilizada, apresentava algumas limitações. Parte dessas limitações foram resolvidas na versão 3, definida pela RFC 1813 (CALLAGHAN; PAWLOWSKI; STAUBACH, 1995). Em 1996, a Sun tentou criar uma versão do protocolo NFS que pudesse ser utilizada através da Internet, chamada de *WebNFS* e definida nas RFCs 2054 (CALLAGHAN, 1996a) e 2055 (CALLAGHAN, 1996b), porém sem sucesso.

Quando as versões 2 e 3 do NFS foram projetadas, a Internet não era tão popular e a segurança não era um fator tão importante quanto hoje, de forma que essas versões eram voltadas apenas para uso em redes locais Unix. Para que a nova versão do protocolo pudesse se adaptar bem ao uso em um ambiente inseguro como a Internet, muitas mudanças foram necessárias. Diante disso, sob o controle do IETF[1] (*Internet Engineering Task Force*), em dezembro de 2000 foi publicada a RFC 3010 (SHEPLER *et al.*, 2000) que apresenta a versão 4 do NFS. Após ser revisada, com o objetivo de facilitar a implementação do novo protocolo, em abril de 2003 foi publicada a RFC 3530 (SHEPLER *et al.*, 2003).

O objetivo deste artigo é apresentar as principais características do NFSv4, bem como apresentar uma reflexão crítica sobre sua evolução a partir da comparação com o modelo mais comum de desenvolvimento de software livre. Não serão tratados detalhes de instalação e configuração do NFSv4 no Linux, uma vez que as informações sobre as particularidades de cada distribuição podem ser obtidas na página de Internet dos desenvolvedores da implementação.

[1] http://www.ietf.org/

2. Principais Características

Muitas mudanças ocorreram na arquitetura da versão 4 do NFS. Em virtude da época de desenvolvimento das versões anteriores, muitos conceitos atuais exigiram a reestruturação do protocolo, como a popularidade da Internet e conseqüentemente a segurança. As principais características da nova versão são apresentadas a seguir:

2.1. Pseudo-Sistema de Arquivos

A introdução do conceito de um sistema de arquivos virtual, ou pseudo-sistema de arquivos (*pseudofilesystem*), permite que o administrador exporte partes não contíguas do sistema de arquivos, de forma transparente ao usuário, ou seja, para ele, as partes exportadas apresentam-se como um único espaço de nomes. Esse novo conceito elimina a inconsistência de uma representação estática, tornando possível aos usuários navegarem pelo sistema de arquivos virtual.

Dessa forma, um servidor que exporta diversos sistemas de arquivos (ou diretórios), deve ligá-los entre si em um único pseudo-sistema de arquivos, formando uma raiz comum. No Linux, o pseudo-sistema de arquivos pode ser considerado um sistema de arquivos real. Com isso os clientes realizarão as pesquisas nele, através do caminho da raiz montada em algum ponto do sistema de arquivos local.

É importante notar que o administrador tem liberdade para montar determinada parte do sistema de arquivos local onde lhe for conveniente. Qualquer parte do sistema de arquivos real, pode ser ligada a qualquer parte do sistema de arquivos virtual, muitas vezes simplificando o acesso e eliminando caminhos desnecessários.

2.2. Listas de Controle de Acesso (ACLs)

Um significante atributo adicionado ao NFSv4 são as Listas de Controle de Acesso (*Access Control Lists* ou ACLs), proporcionando mais liberdade ao administrador do sistema. Os sistemas Unix baseiam suas permissões de arquivos em um atributo de 9 bits, que indicam os tipos de acesso (`r, w, x, -`) para o proprietário do arquivo (ou diretório), grupo do qual ele faz parte e usuários pertencentes a outros grupos. Esse é um sistema muito simples e eficiente para grande parte dos usuários, porém é limitado.

Em alguns casos é necessário definir um controle de acesso mais específico. As ACLs garantem essa liberdade, permitindo definir para cada usuário ou grupo, quais os direitos que cada um deles têm sobre determinado arquivo ou diretório. O uso de ACLs evita, por exemplo, a necessidade de criação de grupos apenas para tratar casos excepcionais, uma prática comum para os administradores de sistemas Unix. Uma ACL é simplesmente uma lista que descreve quais usuários e grupos têm acesso a determinado arquivo e qual o tipo de acesso.

O conjunto de ACLs nativas do padrão POSIX permite apenas dois tipos de entradas, ALLOW e DENY, permitindo ou proibindo o acesso, respectivamente. O conjunto definidas na RFC 3530 é baseado no Microsoft Windows NT, permitindo, além dos dois tipos já citados, as entradas AUDIT e ALARM, que permitem ao sistema efetuar registro (*log*) das operações sobre o arquivo e gerar alarmes no sistema, respectivamente.

2.3. Segurança

Uma das maiores mudanças estruturais do NFSv4 em relação aos seus antecessores é a eliminação dos protocolos subordinados, fazendo dele um protocolo único e que utiliza

portas bem definidas, facilitando sua operação e uso através de *firewalls*. Além disso, na versão 4 do NFS, o arcabouço RPCSEC_GSS, definido na RFC 2203 (EISLER; CHIU; LING, 1997), é utilizado para estender a segurança básica do RPC. Com ele, vários mecanismos podem fornecer serviços de autenticação, integridade e privacidade, como Kerberos, definido na RFC 1510, SPKM-3 e LIPKEY, definidos na RFC 2847.

Os serviços de criptografia são oferecidos pela GSS-API (*Generic Security Service Application Program Interface*), definida na RFC 2743 (LINN, 2000), que permite o uso de vários mecanismos de segurança, incluindo o Kerberos V5 (KOHL; NEUMAN, 1993), LIPKEY e SPKM-3 (EISLER, 2000), além do tradicional AUTH_SYS[2].

A versão 4 do NFS baseia-se em *strings* codificadas pelo padrão UTF-8, para expressar proprietários e grupos no formato `usuario@dominio` e `grupo@dominio`, sendo que a parte `@dominio` é opcional. Para que essa representação seja possível, é necessária uma tradução entre os números *UID/GID* e as *strings* no formato UTF-8. Bases de dados remotas, como NIS (*Network Information Server*) ou LDAP (*Lightweight Directory Access Protocol*), podem ser utilizadas para realizar essa tradução. Uma outra forma de se fazer isso é através de um *daemon* do espaço de usuários, o `GSSD`.

Com o Kerberos V5 é possível utilizar três níveis de segurança, krb5, krb5i e krb5p (autenticação, integridade e privacidade, respectivamente).

O motivo do NFSv4 não utilizar SSL (*Security Socket Layer*), é que em primeiro lugar esse mecanismo não é capaz de suportar comunicação não orientada à conexão, como por exemplo o protocolo UDP, uma vez que o padrão do NFSv4 prevê sua capacidade de trabalhar sobre esse tipo de protocolo. Outro motivo é que o protocolo RPC possui sua própria arquitetura de segurança e não seria muito simples integrar um com outro. O RPCSEC_GSS fornece segurança equivalente ao SSL e ainda é compatível com outros mecanismos, como o AUTH_SYS.

3. Implementação do NFSv4 para Linux

Um grupo do *Center for Information Technology Integration - CITI*[3], da Universidade de Michigan é o principal responsável pela implementação do NFSv4 para uso no Linux.

A implementação do NFSv4 desenvolvida pelo CITI, ainda não incorpora todas as funcionalidades estabelecidas pela RFC 3530, mas as principais já podem ser utilizadas com certa segurança e estabilidade. As distribuições Linux mais populares como Fedora Core e Debian já disponibilizam os pacotes necessários e oferecem o suporte habilitado por padrão no *kernel*.

O suporte ao mecanismo SPKM-3 (*Simple Public Key Mechanism 3*) ainda não está completo. Apesar de existir uma versão experimental para este mecanismo, que atua no espaço do *kernel*, muita coisa ainda deve ser implementada na biblioteca que atua no espaço de usuários. O mecanimo LIPKEY (*Low Infrastructure Public Key*) depende do SPKM-3, mas o CITI afirma que não será uma tarefa difícil adicionar suporte a ele, desde que o SPKM-3 seja suportado (CITI, 2005).

A inclusão de suporte para IPv6 teve seu desenvolvimento iniciado recentemente

[2] AUTH_SYS é também conhecido como AUTH_UNIX

[3] `http://www.citi.umich.edu/projects/nfsv4/`

pelo grupo de projetos da Bull Corporate[4], mas *patches* relacionados ao IPv6 para o cliente já podem ser encontrados. Muitas das funcionalidades especificadas pelo padrão já encontram-se em operação nas suas versões mais recentes, porém novos recursos ainda são aguardados, como um suporte mais completo a ACLs e sua aplicação em sistemas de arquivos paralelos.

Um fato a ser considerado é que a RFC 3530 prevê o uso do NFSv4 sobre protocolos de transporte não orientados à conexão, como o UDP, uma vez que ele foi estruturado de forma a não exigir chamadas de retorno. Já a implementação do NFSv4 desenvolvida pelo CITI não considera esse tipo de protocolo a fim de garantir uma melhor confiabilidade através da Internet, invalidando o uso do NFSv4 sobre o protocolo UDP. Esse assunto será melhor detalhado mais adiante neste documento.

4. Cessão do Controle do NFS ao IETF - RFC 2339

Publicada em Maio de 1998, a RFC 2339 (THE INTERNET SOCIETY AND SUN MICROSYSTEMS, 1998) não trata-se de uma especificação de padrão para a Internet, mas sim de um acordo entre a Sun Microsystems e a Internet Society, sendo conduzida pelo IETF.

Este acordo visa garantir que a especificação do NFS, até então sob total controle da Sun Microsystems e protegida pelas leis de patentes, fosse transferida a uma comunidade internacional e aberta de projetistas e pesquisadores interessados na evolução da arquitetura da Internet, livres de qualquer interesse individual. Diante disso, pode-se deduzir que este foi o primeiro passo da empresa rumo a um modelo de desenvolvimento mais aberto e mais próximo do software livre. Além disso, esse fato pode ser relacionado ao modelo bazar, idealizado por Eric S. Raymond, em (RAYMOND, 2001).

Os termos deste acordo abrangem as condições necessárias para que o controle da especificação do protocolo pudesse ser transferido a uma comunidade aberta. Entre muitas condições citadas no documento, as principais se referem aos direitos autorais e direitos de patente, essenciais à especificação de um padrão aberto. Além dessas condições, é abordado também que para o propósito deste acordo, a Sun Microsystems tornaria disponível informações sobre o ponto inicial para o desenvolvimento da especificação da versão 4 do NFS.

Neste ponto é muito importante esclarecer que o acordo firmado na RFC 2339 trata do controle da especificação do protocolo e não da implementação do código em si. Um exemplo disso é que antes mesmo desse acordo ser estabelecido, já era possível que o NFS fosse implementado sem a intervenção da Sun Microsystems, porém, os direitos de alteração na especificação ou criação de produtos derivados do protocolo eram exclusivos de sua proprietária.

5. Discussão

O fato da Sun Microsystems ter cedido o controle do NFS ao IETF contribui para que o NFSv4 torne-se um protocolo forte e amplamente utilizado. Com isso espera-se que inúmeros desenvolvedores de sistemas operacionais, sejam eles livres ou proprietários,

[4] `http://www.bullopensource.org`

adotem esse protocolo em suas distribuições. Isso permite que administradores de sistemas heterogêneos tenham a opção de adotar uma solução única, aberta, forte e segura para o compartilhamento de arquivos.

De acordo com a RFC 3530, os procedimentos COMPOUND (compostos) foram incluídos para melhorar o desempenho em redes com grande latência. A latência cumulativa, ocasionada por um alto número de chamadas, é evitada agrupando-se várias operações em uma única requisição. Entretanto, em testes realizados com a ferramenta `nfsstat`, responsável por apresentar as estatísticas do protocolo, verificou-se que o número de chamadas aumentou em relação à versão anterior. Apenas um estudo mais aprofundado pode indicar as causas desse fato.

Uma questão polêmica é o uso do NFSv4 sobre o protocolo UDP. A RFC 3530 não cita explicitamente o suporte a este protocolo, mas ela se refere sobre o suporte a protocolos não orientados à conexão, categoria que engloba o UDP. Como é sabido, este protocolo possui várias deficiências, pois trata-se de um mecanismo não confiável, sem controle de fluxo e suas mensagens possuem tamanho limitado. Outro problema surge quando ele é utilizado sob altas taxas de transferência, pois os dados corrompidos não podem ser identificados. Por esses motivos, como já foi citado anteriormente, o CITI optou por não incluir o suporte ao UDP em sua implementação. Mesmo assim existem estudos sobre a utilização do NFSv4 sobre o protocolo UDP, pois o objetivo destes experimentos é a melhoria no desempenho do NFS.

Apesar das questões relacionadas aos protocolos não orientados à conexão, existe um esboço intitulado ”RDMA Transport for ONC RPC”(http://www.ietf.org/internet-drafts/draft-ietf-nfsv4-rpcrdma-02.txt). RDMA é uma nova técnica para uma eficiente movimentação de dados entre dois nós finais, os quais podem aumentar a velocidade utilizada na comunicação. De acordo com o esboço, esta técnica deve ser utilizada em conjunto com as ONC RPC (Open Network Computing RPC), mais conhecidas como RPC versão 2 e definidas pela RFC 1831, que por sua vez pode ser utilizada tanto sobre o protocolo TCP como pelo protocolo UDP.

O NFS, até sua versão 3, apesar de ter suas especificações abertas, era um padrão proprietário, ou seja, apenas a Sun Microsystems tinha permissão para alterá-las e assim definir o rumo do desenvolvimento desta tecnologia. Depois da cessão do padrão à uma comunidade aberta e sem interesses individuais, muitas questões e novas idéias surgiram, mesmo que algumas vezes em desacordo com o padrão, fatos esses, praticamente impossíveis de ocorrerem em um padrão proprietário.

6. Conclusão

De acordo com o que foi apresentado neste trabalho, observamos que a versão 4 do NFS tem um futuro promissor. Isso deve-se ao fato que, por tratar-se de um protocolo aberto, desenvolvido nos moldes do software livre, muitas características podem ser alteradas no próprio protocolo ou então originar produtos derivados. As discussões abertas entre projetistas e desenvolvedores de uma comunidade internacional, prova que um modelo de desenvolvimento mais aberto somente tem a acrescentar em termos de qualidade de um padrão de serviço.

Referências

CALLAGHAN, B. *WebNFS Client Specification*. Internet Engineering Task Force (IETF), out. 1996. (Request for Comments: 2054). Disponível em: <http://www.ietf.org>.

CALLAGHAN, B. *WebNFS Server Specification*. Internet Engineering Task Force (IETF), out. 1996. (Request for Comments: 2055). Disponível em: <http://www.ietf.org>.

CALLAGHAN, B.; PAWLOWSKI, B.; STAUBACH, P. *NFS Version 3 Protocol Specification*. Internet Engineering Task Force (IETF), jun. 1995. (Request for Comments: 1813). Disponível em: <http://www.ietf.org>.

CITI. *FAQs about CITI's Linux NFSv4 Implemention*. 20 nov. 2005. WWW. Disponível em: <http://www.citi.umich.edu/projects/nfsv4/linux/faq/>.

EISLER, M. *LIPKEY - A Low Infrastructure Public Key Mechanism Using SPKM*. Internet Engineerig Task Force (IETF), jun. 2000. (Request for Comments: 2847). Disponível em: <http://www.ietf.org>.

EISLER, M.; CHIU, A.; LING, L. *RPCSEC_GSS Protocol Specification*. Internet Engineering Task Force (IETF), set. 1997. (Request for Comments: 2203). Disponível em: <http://www.ietf.org>.

KOHL, J.; NEUMAN, C. *The Kerberos Network Authentication Service (V5)*. Internet Engineering Task Force (IETF), set. 1993. (Request for Comments: 1510). Disponível em: <http://www.ietf.org>.

LINN, J. *Generic Security Service Application Program Interface - Version 2, Update 1*. Internet Engineering Task Force (IETF), jan. 2000. (Request for Comments: 2743). Disponível em: <http://www.ietf.org>.

RAYMOND, E. S. *The Cathedral and the Bazaar*. Sebastopol: O'Reilly, 2001. Disponível em: <http://www.catb.org/ esr/writings/cathedral-bazaar/cathedral-bazaar/>.

SHEPLER, S.; CALLAGHAN, B.; ROBINSON, D.; THURLOW, R.; BEAME, C.; EISLER, M.; NOVECK, D. *NFS version 4 Protocol*. Internet Engineering Task Force (IETF), dez. 2000. (Request for Comments: 3010). Disponível em: <http://www.ietf.org>.

SHEPLER, S.; CALLAGHAN, B.; ROBINSON, D.; THURLOW, R.; BEAME, C.; EISLER, M.; NOVECK, D. *Network File System (NFS) version 4 Protocol*. Internet Engineering Task Force (IETF), abr. 2003. (Request for Comments: 3530). Disponível em: <http://www.ietf.org>.

SUN MICROSYSTEMS INC. *NFS: Network File System Protocol Specification*. Internet Engineering Task Force (IETF), mar. 1989. (Request for Comments: 1094). Disponível em: <http://www.ietf.org>.

THE INTERNET SOCIETY AND SUN MICROSYSTEMS. *An Agreement Between the Internet Society, the IETF, and Sun Microsystems, Inc. in the matter of NFS V.4 Protocols*. Internet Engineering Task Force (IETF), maio 1998. (Request for Comments: 2339). Disponível em: <http://www.ietf.org>.