



28 · 29 · 30
de OUTUBRO

XII SEGET
SIMPÓSIO DE EXCELÊNCIA EM GESTÃO E TECNOLOGIA
TEMA 2015
Otimização de Recursos e Desenvolvimento



análise de ferramentas de transferência para grandes volumes de dados

Rômulo Alceu Rodrigues
romulo.rodrigues@cptec.inpe.br
INPE

Eugênio Sper de Almeida
eugenio.almeida@cptec.inpe.br
INPE

Resumo: Nos últimos anos os satélites, sensores e supercomputadores passaram a gerar imensas quantidades de dados: imagens em alta resolução, resultados de simulações, dados de experimentos e observações, arquivos texto, etc.. A natureza destes recursos faz com que na grande maioria dos casos estejam distribuídos geograficamente, o que implica na utilização de diversos tipos de tecnologias para transferência de dados por grandes distâncias. Embora existam ferramentas e protocolos modernos, ainda há casos de utilização de protocolos como o File Transfer Protocol (FTP) por algumas instituições, que além de oferecer baixa performance quando comparado a alternativas modernas oferece graves riscos a segurança de informação. Este trabalho analisa um caso de uso aplicado no Centro de Previsão de Tempo e Estudos Climáticos do Instituto Nacional de Pesquisas Espaciais e faz um estudo comparativo entre as ferramentas wget, axel, scp, scp-hpn, sftp, aria2c e gridftp demonstrando que a escolha de ferramentas adequadas têm impacto positivo nas transferências em ambientes científicos. Os testes realizados consistiram em transferir um dado meteorológico de 3.5Gb entre dois equipamentos conectados a uma rede 10Gbps, isolados do tráfego corporativo. Os resultados demonstraram que a diferença no tempo de transferência é de até 92%.

Palavras Chave: redes - desempenho - ferramentas - transferências - grandes volumes



28 · 29 · 30
de OUTUBRO

XII SEGET
SIMPÓSIO DE EXCELÊNCIA EM GESTÃO E TECNOLOGIA
TEMA 2015
Otimização de Recursos e Desenvolvimento



1. INTRODUÇÃO

O grande volume de dados produzido diariamente por instituições científicas, utilizando instrumentos e/ou modelos computacionais, tende a ter vida longa e estar publicamente acessível com o objetivo de análise contínua (HEY et al., 2009). A origem destes dados pode ser um sensor, satélite, supercomputador ou outro dispositivo. Seu destino é quase sempre um ou mais datacenters, onde ficam localizados os sistemas de armazenamento.

As medidas de transferência e armazenamento de dados no dia a dia de um ambiente de TI mudaram rapidamente passando de Gigabytes para Terabytes e até Petabytes em períodos que variam entre semanas, dias e até horas ou minutos. Tais mudanças representam um enorme desafio as organizações que procuram cada vez mais rever suas tecnologias e arquiteturas de redes e armazenamento para que os usuários tenham acesso a essas informações de forma eficiente.

Conhecer e implementar uma infraestrutura computacional apropriada em conjunto com as ferramentas de transferência de dados adequadas para este cenário é de extrema importância para que as expectativas das instituições quanto ao desempenho e segurança da transferência de seus dados sejam atingidos.

As redes de comunicação de dados são essenciais para garantir o transporte rápido e seguro de dados por distâncias que variam desde prédios em um mesmo campus até continentes, a pesquisa que no passado era desenvolvida de uma forma mais local rapidamente adotou uma natureza colaborativa em escala global.

Dentre os inúmeros desafios enfrentados neste ambiente estão o crescimento exponencial dos datasets nos últimos anos, as políticas de acesso aos dados de cada instituição, a movimentação dos dados em janelas de tempo cada vez mais restritas. O fator humano tem seu impacto, uma vez que nem sempre as equipes de tecnologia da informação e os usuários conseguem se entender em qual a solução mais adequada e segura para resolver seu problema. Há também os desafios técnicos que envolvem a arquitetura de redes aplicada e as ferramentas de transferência utilizadas, que podem criar um gargalo adicional.

Nos últimos anos, a arquitetura de redes tradicional que normalmente utiliza um firewall de estado de conexão para filtrar o tráfego entre redes se mostrou adequada a maioria dos ambientes. No entanto, novas aplicações (muitas vezes não testadas) trouxeram novas ameaças, e o grande numero de conexões e usuários externos que se conectam a infraestrutura computacional através de *Virtual Private Networks* (VPN) ou outro meio de acesso externo cresceu junto com a demanda por desempenho e usabilidade. Algumas instituições ainda utilizam ferramentas ultrapassadas e inseguras para transferir seus dados, criando um risco desnecessário á segurança da informação, visto que já existem alternativas que apresentam desempenho e segurança superiores no mercado.

A arquitetura tradicional não apresenta um desempenho satisfatório quando aplicado no ambiente científico que requer transferências de grandes volumes em alta velocidade.



28 · 29 · 30
de OUTUBRO

XII SEGET
SIMPÓSIO DE EXCELÊNCIA EM GESTÃO E TECNOLOGIA
TEMA 2015
Otimização de Recursos e Desenvolvimento



Neste tipo de ambiente o tráfego geralmente ocorre entre equipamentos e aplicações conhecidas e desde que devidamente isolado não existe ou pelo menos não deveriam existir fatores complicadores como servidores liberados para acesso público via Internet e acesso de usuários externos nesta rede.

Em uma série de estudos realizados recentemente pela *Energy Sciences Network* (EsNet), órgão do Departamento de Energia americano dedicado ao suporte à pesquisa na instituição, conclui-se que os firewalls de estado de conexão contribuem negativamente neste caso, principalmente quando as transferências ocorrem entre grandes distâncias e envolvem grandes volumes. O estudo propõe a utilização de um ambiente isolado e customizado para grandes transferências, utilizando Access Control Lists (ACL) implementadas em roteadores, monitoramento adequado dos recursos, ferramentas adequadas e servidores otimizados para este uso específico (ESNET, 2015).

Um dos grandes produtores de dados científicos são os centros meteorológicos, cujo objetivo é melhorar a observação, a compreensão e a previsão do comportamento da atmosfera. Disseminar esse conhecimento de forma rápida e ampla, e orientar a comunidade na sua utilização permite que um grande número de decisões diárias sensíveis às condições meteorológicas possam ser feitas no melhor interesse do bem-estar econômico e social do país, em todas as esferas da vida (MASON, 1996).

O Centro de Previsão de Tempo e Estudos Climáticos (CPTEC), pertencente ao Instituto Nacional de Pesquisas Espaciais (INPE), tem a missão de disponibilizar ao Brasil o estado da arte em previsões atmosféricas (tempo, clima e qualidade do ar). Para isto busca constantemente o aprimoramento de sua capacidade científica e tecnológica, visando a melhoria continuada das previsões meteorológicas para a trazer benefícios da sociedade.

As informações meteorológicas utilizadas e produzidas pelos modelos atmosféricos do INPE/CPTEC são caracterizadas pelo seu grande volume de dados diários. Necessitam de enlaces de dados de alta velocidade e mecanismos eficientes para a transferência de dados.

Este trabalho visou avaliar ferramentas de transferência de dados, com o intuito de identificar a mais adequada para transferência de dados meteorológicos entre instituições utilizando conexões de 10Gbps. Para esta finalidade foram analisadas as ferramentas wget, axel, scp, scp-hpn, sftp, aria2c e globus-url-copy (GridFtp).

Os equipamentos e ferramentas foram instalados no perímetro da rede corporativa e conectados diretamente ao *backbone* da RNP a 10 Gbps. Esta abordagem eliminou a concorrência com o tráfego de outras aplicações da rede corporativa que opera a 1 Gbps.

2. PROTOCOLOS DE TRANSFERÊNCIA DE DADOS

Um protocolo define o formato de dados que é enviado entre dois sistemas, incluindo a sintaxe das mensagens, o conjunto de caracteres e o sequenciamento da mensagem. Seu grande valor é prover interoperabilidade (Allcock, 2000).



28 · 29 · 30
de OUTUBRO

XII SEGET
SIMPÓSIO DE EXCELÊNCIA EM GESTÃO E TECNOLOGIA
TEMA 2015
Otimização de Recursos e Desenvolvimento



Um protocolo de transferência de dados é definido considerando que um computador é o transmissor de um fluxo de mensagens e o outro o receptor (STENNING, 1976). São disponibilizados em serviços, que são processos que usualmente são inicializados automaticamente (sempre em execução) e que provêm funcionalidades básicas para outras aplicações.

A transferência de dados é muito comum para o intercâmbio de dados, que pode ter um volume de dados variável (bytes a terabytes), podendo ser entre recursos computacionais geograficamente distribuídos ou em uma rede local.

A arquitetura cliente-servidor é adotada na implementação dos serviços de transferência de dados e atualmente existem diversos protocolos que são utilizados para transferência de dados.

2.1 FILE TRANSFER PROTOCOL (FTP)

A proposta inicial do protocolo FTP (File Transfer Protocol) foi publicada na Request for Comments (RFC) 114 (Bhushan, 1971). Ocorreram diversas atualizações desde sua criação e ainda é utilizado por muitas instituições para disponibilizar ou transferir dados.

O FTP teve sua origem em uma época na qual a Internet era composta por um pequeno e conhecido conjunto de equipamentos, que necessitavam transferir pequenos arquivos entre si. Preocupações com a segurança da informação não era um fator crítico nesta rede. Desta forma, o protocolo não foi projetado para funcionar em conjunto com Network Address Translation (NAT) ou firewalls (OPENBSD, 2015).

A implementação do protocolo FTP é baseada *Transmission Control Protocol* (TCP) e funciona nos modos ativo e passivo. Ambos utilizam dois (2) canais de comunicação entre o cliente e o servidor, separados em duas conexões TCP: canal de comandos e de dados.

O modo ativo funciona com o cliente abrindo o canal de controle (porta 21) ao servidor e informando ao servidor para conectar em uma porta aleatória maior que 1023. Este modo impacta a segurança, pois neste caso a conexão de transferência é iniciada a partir do servidor.

O modo passivo é considerado mais seguro pois todas as conexões são iniciadas pelo cliente. Neste caso, as chances de uma conexão comprometida são menores. O cliente abre uma conexão de controle na porta 21 ao servidor. O servidor concorda e informa uma porta de conexão aleatória maior que 1023.

2.2 Secure Shell (SSH)

O Secure Shell (ssh) surgiu como forma de prevenir o *password sniffing*, devido a um caso real de ataque na Helsinki University of Technology na Finlândia (Barrett e Silverman, 2001). Na época era uma opção segura aos protocolos não seguros disponíveis: rlogin, rsh, and rcp.



28 · 29 · 30
de OUTUBRO

XII SEGET
SIMPÓSIO DE EXCELÊNCIA EM GESTÃO E TECNOLOGIA
TEMA 2015
Otimização de Recursos e Desenvolvimento



As transferências de dados com ssh possuem a vantagem da segurança da senha e dos dados, que trafegam por um túnel criptografado. A utilização de uma única porta para conexão facilita sua utilização em ambientes protegidos por firewalls e NAT.

Adicionalmente ao mecanismo tradicional de autenticação por meio de senhas, o ssh possui a opção de utilização de chaves públicas que aumenta a segurança (desde que o controle de chaves seja feito corretamente). Nesse caso o funcionamento se baseia em duas chaves: pública e privada. A chave pública é instalada no servidor de destino e a chave privada é utilizada no cliente, não sendo possível reconstruí-la somente a partir da chave pública (VANDYKE, 2008).

2.3 *Globus File Transfer Protocol (GridFTP)*

O protocolo surgiu da GridFtp necessidade de estabelecimento de um padrão para transferências de grandes volumes de dados na Internet entre instituições científicas. Ele foi implementado pela *Globus Alliance* e é recomendado pela *Global Grid Forum*.

O GridFtp consiste em um conjunto de extensões ao FTP e originalmente era distribuído como parte do Globus Toolkit, pacotes de ferramentas para implementação de ambientes de Grid (BUTLER, 2010).

Suas funcionalidades incluem: negociação automática dos buffers TCP e Window Size, transferência de dados paralela, transferências parciais de arquivos, transferência de dados distribuída, funcionalidades de segurança e mecanismos de tolerância a falhas.

3. FERRAMENTAS PARA TRANSFERÊNCIA DE DADOS

Este estudo de caso baseou-se principalmente na camada de aplicação, utilizando ferramentas que utilizam os protocolos FTP, SSH e GridFTP: wget, axel, scp, scp-hpn, aria2c e gridftp.

O wget (<http://www.gnu.org/software/wget/>) é uma ferramenta muito utilizada em ambientes Linux/Unix, portanto um candidato natural para ser avaliado. Surgiu em um momento que houve a popularidade da Internet e foi desenvolvida para funcionar em enlaces de dados lentos e não confiáveis (Anglano, C.; Canonico, 2004).

Na época de seu desenvolvimento não havia uma ferramenta que suportasse os protocolos ftp e http. A robustez do Wget é caracterizada por sua versatilidade e capacidade de se recuperar de falhas na rede. Suas funcionalidades incluem: recursividade (a ferramenta permite a clonagem de websites inteiros), modo não interativo, uso de filtros, suporte a proxies, etc..

A ferramenta axel (<http://freecode.com/projects/axel>) permite tanto a transferência de dados de múltiplos servidores FTP (multi-conexão) como uma simples transferência utilizando múltiplos fluxos ao mesmo tempo, aumentando a velocidade de transferência. Seu ponto fraco é a falta de suporte a autenticação.



28 · 29 · 30
de OUTUBRO

XII SEGET
SIMPÓSIO DE EXCELENCIA EM GESTÃO E TECNOLOGIA
TEMA 2015
Otimização de Recursos e Desenvolvimento



O scp (<http://www.openssh.com>) é uma ferramenta utilizada para transferência segura de arquivos, bastante utilizada em ambientes Unix/Linux. Baseado no antigo protocolo Rate Control Protocol (RCP), o scp utiliza o protocolo SSH para realizar transferências de arquivos de modo seguro (Pechanec, 2007). No entanto, ela possui problemas de escalabilidade em ambientes com grandes volumes de transferências devido ao fato dos *buffers* de fluxo de controle serem definidos estaticamente.

A ferramenta scp-hpn (<http://www.psc.edu/index.php/hpn-ssh>) é uma evolução do código da ferramenta scp e do protocolo SSHv2, visando permitir a configuração dos buffers de controle de fluxo automaticamente em tempo de execução. Seu objetivo é resolver problemas relacionados ao baixo desempenho, especialmente em redes de alta capacidade e fluxos de longa duração. A versão original da ferramenta e do protocolo SSHv2 definem estes valores estaticamente, criando um "bottleneck" neste tipo de cenário.

Um teste interessante consiste em aplicar patch scp-hpn que promete aumentar muito o desempenho do scp principalmente em redes de alta velocidade, o que fez com que ambos se tornassem testes mandatórios em nosso cenário. O aria2c (<http://aria2.sourceforge.net>) é uma ferramenta poderosa que oferece recursos como transferências multiprotocolo e multi-conexão, suportando os protocolos http(s), ftp, sftp, bittorrent e metalink.

O aria2c utiliza várias técnicas para obter a velocidade máxima da rede, como o download do mesmo arquivo de várias origens podendo inclusive utilizar protocolos diferentes e múltiplas conexões. O globus-url-copy é uma ferramenta cliente que implementa os protocolos GRIDFTP, FTP, HTTP, HTTPS e FILE (<http://toolkit.globus.org/toolkit/docs/latest-stable/gridftp/user/>). Devido ao seu uso comum no meio científico quando se trata de grandes volumes de dados e seus inúmeros recursos se tornou o último candidato de nossa lista. Existem outros clientes disponíveis para GridFtp, no entanto o grau de personalização oferecido pela globus-url-copy e nossa experiência anterior com a ferramenta foram fatores importantes para que fosse escolhida.

4. METODOLOGIA

O cenário de testes teve como objetivo permitir a comparação entre um conjunto de ferramentas que consideramos ideais para demonstrar os ganhos possíveis de desempenho entre um ambiente corporativo tradicional e um ambiente preparado para transferências de dados. Conforme citado na introdução o conjunto de ferramentas testadas foram wget, axel, sftp, scp, scp-hpn, aria2c e gridftp.

Para a realização das transferências de dados, foram utilizados dois servidores idênticos e otimizados, com a seguinte configuração: dois (2) processadores Intel® Xeon® E5-2640 v3, 128 GB de RAM, oito (8) TB de armazenamento em oito (8) discos de 1TB configurados em RAID 0, 120 GB de armazenamento em disco SSD, e placa de rede de 10Gbps.

Os testes utilizaram um dado meteorológico de 3.5 GBytes em um ambiente livre de concorrência com o tráfego operacional. O objetivo foi simular as transferências de dados



28 · 29 · 30
de OUTUBRO

XII SEGET
SIMPÓSIO DE EXCELÊNCIA EM GESTÃO E TECNOLOGIA
TEMA 2015
Otimização de Recursos e Desenvolvimento



meteorológicos entre o INPE/CPTEC e Instituições parceiras, demonstrando que a utilização de ferramentas adequadas pode representar ganhos significativos no tempo de transferência.

A transferência de dados ocorreu entre esses dois (2) servidores, conectados a um enlace de dados de 10Gbps da Rede Nacional de Pesquisa (RNP). Os servidores foram instalados no CPTEC e na USP-SP, e as ferramentas utilizadas foram wget, aria2c, axel, GridFTP, sftp, scp e scp-hpn. Os testes com axel, aria2c e GridFTP utilizaram um e cinco canais (fluxos paralelos). Os dados históricos do monitoramento indicaram uma banda disponível máxima entre INPE/CPTEC e a USP em torno de 9 Gbps.

Mesmo isolando o ambiente de testes da rede corporativa para evitar problemas de concorrência com outras aplicações e protocolos da rede corporativa, poderia existir impacto com relação a utilização do backbone da RNP, que interconecta as instituições de pesquisa e ensino do Brasil. Para minimizar o impacto deste fator foram realizados testes automatizados em vários horários e dias da semana, a partir dos dados iniciais foi calculada a média de tempo de transferência do arquivo por ferramenta.

Uma das vantagens em se testar a camada de aplicação é que seria muito mais fácil para o usuário usar a ferramenta que melhor atende seus requisitos do que depender de otimizações em camadas inferiores, como a utilização de *Jumbo frames*, alterações nos *buffers* TCP do sistema operacional, alterações na arquitetura de redes da instituição, etc.

5. RESULTADOS

Ferramentas que permitem a transmissão de fluxo paralelos apresentaram menores tempos de transmissão. O melhor tempo de transferência foi de 6s, com a utilização do Gridftp e 5 canais simultâneos. O pior tempo foi utilizando a ferramenta scp-hpn com 1m 14s.

Os resultados abaixo demonstram que a escolha de outras ferramentas mais adequadas para transferência dos dados também reduz os tempos de transmissão reduzindo em até 92% em relação ao wget e scp (Tab. 1) que são ferramentas comumente utilizadas.

Acreditamos que os benefícios deste tipo de estudo ficarão mais evidentes com as futuras melhorias na qualidade dos dados meteorológicos, que acarretarão um aumento na resolução espacial e do tamanho dos dados a serem transferidos pelos centros meteorológicos. Verificou-se principalmente o potencial da utilização de ferramentas adequadas na redução do tempo de transferência de dados. Neste contexto, o estudo demonstrou alternativas para o modelo tradicional de transferência de dados.

Tabela 1: Tempos de transmissão para o cenário de testes.

Ferramenta	Tempo de Transferência	Vazão Média (Gbps)
scp-hpn	00:01:14	0.378
GridFTP	00:01:02	0.452
Wget	00:00:45	0.622



28 · 29 · 30
de OUTUBRO

XII SEGET
SIMPÓSIO DE EXCELÊNCIA EM GESTÃO E TECNOLOGIA
TEMA 2015
Otimização de Recursos e Desenvolvimento



scp	00:00:32	0.875
sftp	00:00:28	1.000
aria2c	00:00:20	1.400
axel	00:00:20	1.400
aria2c (5 canais)	00:00:16	1.750
axel (5 canais)	00:00:15	1.867
GridFTP (5 canais)	00:00:06	4.667

6. CONCLUSÕES

Atualmente, diversas instituições de pesquisa no mundo produzem um grande volume de dados científicos, que são recebidos, processados e disponibilizados por outras instituições. Apesar do crescente aumento da velocidade dos enlaces de dados, diminuir o tempo de transferência de dados é fundamental devido a tendência de crescimento do tamanho dos dados provenientes de aplicações científicas.

Este trabalho visou analisar o desempenho das ferramentas wget, axel, scp, scp-hpn, aria2c e globus-url-copy (GridFtp) em um ambiente isolado do tráfego corporativo para transferências de alto desempenho. No experimento foram utilizados dois (2) servidores otimizados para transferência de dados.

Conclui-se que a utilização de ferramentas e arquiteturas adequadas para transferência de dados proporciona ganhos significativos em comparação com o modelo atual utilizado na instituição. Este estudo demonstrou que a escolha da ferramenta de transferência de dados correta é fundamental, e que pode representar um ganho de até 92%.

7. REFERÊNCIAS

Allcock, W., Foster, I., Tuecke, S., Chervenak, A., & Kesselman, C. Protocols and services for distributed data-intensive science. In AIP Conference Proceedings (pp. 161-163). IOP INSTITUTE OF PHYSICS PUBLISHING LTD, 2000.

Alliance, G. GridFTP-Universal Data Transfer for the Grid. White Paper. 2000.

Anglano, C.; Canonico, M. "A comparative evaluation of high-performance file transfer systems for data-intensive grid applications," Enabling Technologies: Infrastructure for Collaborative Enterprises, WET ICE 2004. 13th IEEE International Workshops on , vol., no., pp.283,288, 14-16 June 2004 doi: 10.1109/ENABL.2004.2, 2004

Barrett, D.; Silverman, R. E. SSH, the Secure Shell: The Definitive Guide, USA: O'Reilly & Associates, 2001.

Bhushan, A., "A File Transfer Protocol", RFC 114 (NIC 5823), MIT-Project MAC, 16 April 1971.

BUTLER, D. Grid FTP Server Simple Performance Measurements. Disponível em: <<http://downloads.bbc.co.uk/rd/pubs/whp/whp-pdf-files/WHP178.pdf>>. Acesso em: 8 mai. 2015.

Butler, D. GRIDFT Server Simple Performance Measurements, BBC R&D White Paper WHP178, <http://www.bbc.co.uk/rd/pubs/whp/whp178.shtml>, 2010



28 · 29 · 30
de OUTUBRO

XII SEGET
SIMPÓSIO DE EXCELÊNCIA EM GESTÃO E TECNOLOGIA
TEMA 2015
Otimização de Recursos e Desenvolvimento



Dart, E.; Rotman, L.; Tierney, B.; Hester, M.; Zurawski, J. The science dmz: A network design pattern for data-intensive science. *Scientific Programming*, 22(2), 173-185, 2014

ENERGY SCIENCES NETWORK; Science DMZ Security - Firewall vs Router ACLs. Disponível em: <<https://fasterdata.es.net/science-dmz/science-dmz-security/>>. Acesso em: 14 mai. 2015.

GAAST, W. ; Axel. Disponível em: <<http://wilmer.gaast.net/main.php/axel.html>>. Acesso em: 10 mai. 2015.

HEY, T.; TANSLEY, S.; TOLLE, K. **The Fourth Paradigm: Data-Intensive Scientific Discovery**, Redmond, WA: Microsoft Research, 2009.

OPENBSD ; PF - Issues with Ftp. Disponível em: <<http://www.openbsd.org/faq/pf/ftp.html>>. Acesso em: 14 mai. 2015.

Pechanec, J. How the SCP protocol works. Weblog post. Jan Pechanec's Weblog, Oracle, 2007

RAPIER, C.; STEVEN, M., BENNET, B., TASOTA, M. High Performance SSH/SCP-HPN-SSH. Disponível em: <<http://www.psc.edu/index.php/hpn-ssh#problem>>. Acesso em: 14 mai. 2015.

STENNING, N. V. A data transfer protocol. *Computer Networks*, v. 1, n. 2, p. 99-110, 1976.

VANDYKE SOFTWARE; An overview of the Secure Shell (SSH). Disponível em: <http://www.vandyke.com/solutions/ssh_overview/ssh_overview.pdf>. Acesso em: 9 jun. 2015.

W. Allcock, J. Bresnahan, R. Kettimuthu, M. Link, C. Dumitrescu, I. Raicu, and I. Foster, "The Globus striped GridFTP framework and server," in SC'05, ACM Press, 2005.