Universidade Federal do Rio de Janeiro

Núcleo de Computação Eletrônica

Maurício Gouvêa Silva

COMPUTAÇÃO EM GRADE:
Aspectos de Segurança

Rio de Janeiro

2006

Maurício Gouvêa Silva

COMPUTAÇÃO EM GRADE:
Aspectos de Segurança

Monografia apresentada para obtenção do título de Especialista em Gerência de Redes de Computadores no Curso de Pós-Graduação Lato Sensu em Gerência de Redes de Computadores e Tecnologia Internet do Núcleo de Computação Eletrônica da Universidade Federal do Rio de Janeiro – NCE/UFRJ.

Orientador:

Prof. Carlos Mendes, NCE, UFRJ, Brasil

Rio de Janeiro

2006

Maurício Gouvêa Silva

COMPUTAÇÃO EM GRADE:
Aspectos de Segurança

Monografia apresentada para obtenção do título de Especialista em Gerência de Redes de Computadores no Curso de Pós-Graduação Lato Sensu em Gerência de Redes de Computadores e Tecnologia Internet do Núcleo de Computação Eletrônica da Universidade Federal do Rio de Janeiro – NCE/UFRJ.

Aprovada em setembro de 2006.

Carlos Mendes

Prof. Carlos Mendes, NCE, UFRJ, Brasil

RESUMO

SILVA, MAURÍCIO GOUVÊA. **COMPUTAÇÃO EM GRADE: Aspectos de segurança**. Monografia (Especialização em Gerência de Redes e Tecnologia Internet). Núcleo de Computação Eletrônica, Universidade Federal do Rio de Janeiro. Rio de Janeiro, 2006.

Estudo sobre os apectos de segurança considerados em implementações de ambientes de computação em grade e os desafios que se apresentam para uma maior disseminação desta tecnologia.

ABSTRACT

SILVA, MAURÍCIO GOUVÊA. **COMPUTAÇÃO EM GRADE: aspectos de segurança**. Monografia (Especialização em Gerência de Redes e Tecnologia Internet). Núcleo de Computação Eletrônica, Universidade Federal do Rio de Janeiro. Rio de Janeiro, 2006.

A work that discusses security aspects involving Grid computing environments implementations and the challenges related to a major use of this technology.

LISTA DE FIGURAS

LISTA DE TABELAS

LISTA DE ABREVIATURAS E SIGLAS

ACL	ACCESS CONTROL LIST
API	APPLICATION PROGRAM INTERFACE
BoT	BAG OF TASKS
CA	CERTFICATION AUTHORITY
CMI	COMMON INFORMATION MODEL
CPU	CENTRAL PROCESSING UNIT
DMTF	DISTRIBUTED MANAGEMENT TASK FORCE
EGA	ENTERPRISE GRID ALLIANCE
GGF	GLOBAL GRID FORUM
GIIS	GRID INDEX INFORMATION SERVICE
GIS	GRID SECURITY INFRASTRUCTURE
GME	GRID MANAGEMENT ENTITY
GRAM	GLOBUS RESOURCE ALLOCATION MANAGER
GRIS	GRID RESOURCE INFORMATION
GSS-API	GENERIC SECURITY SERVICES APPLICATION PROGRAM INTERFACE
IPV4	INTERNET PROTOCOL VERSION 4
IPV6	INTERNET PROTOCOL VERSION 6
LDAP	LIGHTWEIGHT DIRECTORY ACCESS PROTOCOL
MDS	MONITORING AND DISCOVERY SERVICE
NAT	NETWORK ADDRESS TRANSLATION
OASIS	ORGANIZATION FOR THE ADVANCEMENT OF STRUCTURED INFORMATION STANDARDS
OGF	OPEN GRID FORUM
OGSA	OPEN GRID SERVICES ARCHITECTURE
OGSI	OPEN GRID SERVICES INFRASTRUCTURE
PKI	PUBLIC KEY INFRASTRUCTURE
RBAC	ROLE BASED ACCESS CONTROL
RFC	INTERNET ENGINEERING TASK FORCE
RFT	RELIABLE FILE TRANSFER
SAML	SECURITY ASSERTION MARKUP LANGUAGE
SDK	SOFTWARE DEVELOPMENT KIT
SSH	SECURE SHELL
SSL	SECURE SOCKETS LAYER
TLS	TRANSPORT LAYER SECURITY
VO	VIRTUAL ORGANIZATION
W3C	THE WORLD WIDE WEB CONSORTIUM
XACML	EXTENSIBLE ACCESS CONTROL MARKUP LANGUAGE

SUMÁRIO

1 **INTRODUÇÃO**

1.1 MOTIVAÇÃO

Computação em grade (*Grid Computing*) é uma modalidade de processamento distribuído que tem despertado o interesse de inúmeras empresas e instituições em todo o mundo. Ela tem sido considerada base para a virtualização de recursos computacionais e processamento de dados, utilização de banda de rede e capacidade de armazenamento de dados (storage) para criar uma única imagem de sistemas. Com a virtualização, as organizações passam a ter seus sistemas computacionais compartilhados através de redes de comunicação que permitem a colaboração, criando assim "supercomputador virtual" (www.oracle.com/grid). Utilizar máquinas de diferentes redes e usar ciclos ociosos de processamento pode, potencialmente, prover poder computacional similar ao oferecido por supercomputadores (COSTA et al*,* 2004). Formalmente, grades computacionais podem ser conceituadas como plataformas de execução para aplicações paralelas que congregam recursos dispersos geográfica e administrativamente (ARAÚJO et al, 2004). Neste cenário, várias ferramentas têm sido criadas para implementar plataformas de execução de aplicações em grade, com foco tanto no mercado corporativo como na área acadêmico-científica.

A computação em grade cria "pool" de computadores, armazenamento e redes, possibilitando às organizações alocarem recursos dinamicamente, de acordo com suas necessidades. Com o rápido avanço da tecnologia, as organizações podem facilmente adaptar seus recursos de Tecnologia da Informação para o que melhor convier aos seus objetivos.

Segundo Cirne (2003), apesar do grande interesse demonstrado pela academia e pela indústria, a adoção de soluções baseadas em grade ainda é baixa. A computação em grade é considerada um trabalho em progresso (COSTA et al. 2004) e para a sua popularização

algumas limitações tecnológicas precisam ser resolvidas. O tratamento dos requisitos de segurança inerentes a esse tipo de aplicações precisam ser tratados não só para a execução segura de aplicações na grade, mas também para garantir a segurança das instituições que as hospedam. Em ambientes de grade compostos por várias instituições, garantias de segurança são indispensáveis. Do ponto de vista da organização que está compartilhando recursos, é necessário ter o controle sobre o acesso que está sendo efetuado ao seu ambiente. A discussão em torno de um assunto importante e atual como a segurança da informação na computação em grade é, sem dúvida, a grande alavanca deste projeto de pesquisa.

1.2 OBJETIVOS

Para a implementação plena e em larga escala da computação em grade, é essencial que questões relativas à segurança estejam devidamente tratadas e resolvidas. Na prática, nota-se que há um leque razoável de ferramentas de grade, mas algumas não possuem sequer mecanismos de segurança ou apresentam modelos incompletos das mesma. Ao longo desta pesquisa, verificou-se que os grandes desenvolvedores de aplicações para computação em grade (Grid computing) tem focado seriamente na questão da segurança, e as novas versões de suas ferramentas tem apresentado implementações cada vez mais confiáveis neste campo.

Neste contexto, um quesito chave a ser contemplado é o suporte a políticas de autorização. Segundo Welch (2003), um serviço de autorização deve permitir acesso a recursos baseando-se nas informações do requisitante, do recurso a ser acessado e dos detalhes da requisição. Políticas de acesso também são importantes para que a organização que compartilha recursos tenha suas garantias de serviço locais contempladas. O objetivo deste trabalho visa apresentar quais são os atuais requisitos básicos de segurança em computação em grade, estabelecer paralelos entre algumas ferramentas disponíveis nas áreas corporativa e acadêmico-científica, como cada uma delas trata os aspectos relacionados à

segurança, principalmente no que tange ao controle de acesso, e o que podemos vislumbrar para o futuro em termos de confidencialidade e integridade da informação neste tipo de implementação, já que, como foi tratado no início, a virtualização de recursos é o caminho para onde apontam muitas soluções em Tecnologia da Informação.

1.3 RELEVÂNCIA DA PESQUISA

Segurança é, em muitas instituições, uma palavra chave. Uma maior popularização desta tecnologia passa pelo maior entendimento das questões relativas à segurança das redes envolvidas e a informação trocada. Acredito que uma discussão objetiva neste sentido, mesmo não-generalizável, possa trazer resultados relevantes para o futuro.

1.4 ORGANIZAÇÃO

O trabalho está organizado da seguinte forma: No capítulo 2, apresenta-se uma fundamentação teórica de computação em grade e questões relativas à segurança, onde é realizada uma discussão sobre seus aspectos fundamentais e desafios pertinentes. A metodologia usada nesta pesquisa está apresentada no capítulo 3. No capítulo 4 será apresentado o estudo proposto, mostrando quais são os padrões atuais de segurança, implementações comumente usadas no mercado, a apresentação de algumas ferramentas usadas no cenário atual e suas particularidades. O capítulo 5 encerra este trabalho, apresentando as considerações finais e conclusões acerca de qual direção a segurança em computação em grade poderá tomar daqui em diante. Além disso, serão indicados caminhos para a continuidade desta discussão, uma vez que novas vulnerabilidades são descobertas a cada momento e segurança é palavra de ordem para qualquer gestor de redes de computadores.

1.5 LIMITAÇÕES

As limitações evidentes ao método utilizado e a não-generalização dos resultados, pois será a observação do cenário atual de segurança em computação em grade, focado principalmente em seus Forums mais significativos. A percepção do autor, por mais imparcial que tente ser, pode também tornar-se um fator limitador nesta pesquisa.

2 **REFERENCIAL TEÓRICO**

2.1 CONCEITUAÇÃO

A expressão Computação em Grade (*Grid Computing*) foi criada em meados dos anos 90 para denotar uma infra-estrutura de computação distribuída para executar aplicações científicas e de engenharia (FOSTER et al. 2001). Grades, entretanto, possuem características que as diferenciam de outras tecnologias de processamento distribuído. Entre elas, de acordo com (CIRNE, 2003; FOSTER, 2002) pode-se destacar:

- **Heterogeneidade**: uma grade deve ser capaz de congregar equipamentos diferentes entre si, de forma a fazê-los trabalhar em conjunto na execução de uma aplicação;
- **Alta dispersão geográfica**: esta característica se refere ao potencial de utilizar equipamentos que não estão fisicamente próximos, com isso uma grade poderia ser composta por equipamentos de várias partes do mundo;
- **Compartilhamento**: grades devem ser capazes de suportar a execução de várias aplicações simultaneamente;
- **Múltiplos domínios administrativos**: grades podem ser compostas por equipamentos de várias instituições, com administração totalmente independente;
- **Controle distribuído**: tipicamente, não há uma única entidade que tenha o controle sobre toda a grade;
- **Disponibilização de serviços não triviais**: grades devem ser capazes de coordenar a utilização de recursos de forma estruturada, para, assim, atender às necessidades de execução das aplicações; é esperado que a utilidade do sistema combinado (conjunto de recursos alocados) seja significativamente superior à soma de suas partes isoladas.

Essas características, no entanto, propõem um conceito e não uma definição para grades computacionais (CIRNE 2003). Ou seja, uma plataforma que possui as propriedades

acima, certamente poderá ser classificada como grade. Porém, a ausência de alguma das características acima não desqualifica totalmente uma ferramenta dessa nomeação.

A definição de computação em grade está relacionada diretamente com o compartilhamento e uso coordenado de recursos em "Organizações Virtuais" distribuídas. O conceito de "Organização Virtual" (*Virtual Organization* – VO) é largamente utilizado neste cenário, compreendendo grupos de recursos e serviços individuais e associados, unidos por um propósito único, mas não localizados no mesmo domínio administrativo (WELCH et all). O desafio de segurança surge exatamente no que tange à relação de confiança entre entidades, o uso de diversos mecanismos de acesso, a necessidade da criação dinâmica de serviços e a disponibilização da criação dinâmica de "domínios confiáveis".

Características como a heterogeneidade e disponibilização de serviços não triviais dão às grades a capacidade de utilizar, de forma coordenada, os ciclos ociosos de processamento do parque de equipamentos existente. Essa capacidade é, sem dúvida, um grande atrativo para a utilização dessa tecnologia, pois se constitui em uma solução para a obtenção de grande poder computacional, com alta escalabilidade e baixo custo.

Tais características ainda dão o suporte necessário para a virtualização de recursos, ou seja, ter tarefas alocadas a processadores de forma dinâmica. Esta outra propriedade é claramente originada do compartilhamento. Com isto temos os requisitos necessários para a computação sob demanda . Com o paradigma "on demand" de processamento, os recursos são alocados sob demanda, em função das necessidades de processamento em determinado momento. No momento em que uma determinada tarefa exigir mais processamento, novos equipamentos podem ser alocados para a grade.

Na maioria das vezes a computação em grade é relacionada à obtenção de poder computacional. Entretanto, grades também podem ser criadas para o compartilhamento de dados, os chamados *Data Grids* (GRID CAFÉ 2004). Grades de dados, assim, provêem acesso transparente, seguro e de alta performance a conjuntos de dados entre diferentes domínios administrativos e organizações. Grades também podem ser classificadas quanto ao seu escopo de atuação. Assim, grades departamentais (*Departamental Grids*) são utilizadas por uma área determinada de uma organização; grades empresariais (*Enterprise Grids*) objetivam prover serviços aos funcionários de uma organização; grades inter-empresas (*Extraprise Grids*) estabelecem grades entre companhias; e grades globais (*Global Grids*) que se constituem em grades construídas sobre a Internet e potencialmente estão acessíveis a várias instituições ao redor do mundo.

Grades, por serem ferramentas de execução paralela também devem considerar questões pertinentes a este paradigma de desenvolvimento, como o modelo de programação a ser utilizado (troca de mensagens ou memória compartilhada), balanceamento de carga e tolerância à falhas. Por suas características de alta heterogeneidade e de ampla distribuição, grades também trazem uma nova gama de aspectos a serem considerados (CIRNE 2003). São necessários, por exemplo, serviços capazes de prover segurança fim-a-fim, na medida em que os dados poderão trafegar em redes não conhecidas. São necessários também mecanismos para gerenciamento de aplicações, capazes de alocar, escalonar e contabilizar a utilização de recursos.

2.2 GERENCIADORES DE RECURSO E ESCALONADORES

Segundo Carvalho (2005), *Middleware* é o neologismo criado para designar camadas de software que não constituem diretamente aplicações, mas que facilitam o uso de ambientes ricos em tecnologia da informação. A camada de *middleware* concentra serviços como identificação, autenticação, autorização, diretórios, certificados digitais e outras ferramentas para segurança. Aplicações tradicionais implementam vários destes serviços, tratados de forma independente por cada uma delas. As aplicações modernas, no entanto, delegam e centralizam estes serviços na camada de *middleware*. Ou seja, o *middleware* serve como elemento que aglutina e dá coerência a um conjunto de aplicações e ambientes.

Uma das atribuições de um *middleware* de grade é realizar a alocação de recursos. Assim, o *middleware* é responsável por enviar as tarefas para execução nos processadores da grade. O componente responsável por executar esta tarefa é chamado de escalonador. Pode-se dizer que o escalonamento de recursos na computação em grade enfrenta vários desafios. Muitas vezes, os recursos que compõem a grade pertencem a instituições diferentes, sendo assim inaceitável que tais recursos sejam controlados por apenas uma entidade. O ideal, segundo (ARAÚJO et al, 2004), é que a responsabilidade de escalonamento seja dividida entre as instituições. O estado da arte na solução deste tipo de problema, segundo (CZAJKOWSKI et al, 2001) e (ARAÚJO et al, 2004) é a criação da figura de gerenciadores de recursos ou escalonadores de recursos.

O gerenciador de recursos controla o conjunto de recursos que faz parte da grade. Grades devem ser capazes de utilizar vários gerenciadores de recursos. Analisando grades compostas de mais de um domínio administrativo, poderia-se pensar em uma arquitetura onde cada instituição possuísse um ou mais gerenciadores de recurso.

Com isso, se tem a subdivisão entre escalonadores de aplicação e escalonadores de recursos. Escalonadores de aplicação, assim, são responsáveis apenas pela execução das aplicações na grade. Eles não controlam recursos, apenas os solicitam aos escalonadores de recursos. Assim, a principal responsabilidade dos escalonadores de aplicação é dividir as tarefas e encaminhá-las aos processadores alocados. Esta estratégia é adotada em várias ferramentas de grade, como, por exemplo, o Globus e a suíte MyGrid/OurGrid.

2.3 ORGANIZAÇÕES

Conforme descrito na seção anterior, uma das características mais marcantes da computação em grade é a sua capacidade de lidar com a heterogeneidade dos equipamentos que a compõem. Grades devem também ser capazes de comunicar-se entre si. Esta integração é claramente desafiadora, quando se considera que grades diferentes são controladas por organizações independentes, que não compartilham a mesma administração, as mesmas políticas ou as mesmas ferramentas.

Para facilitar este tipo de interconexão, tem-se claramente a necessidade de padronização ou recomendação de arquiteturas em ambientes de computação em grade. Este é o objetivo de algumas organizações, verdadeiros Forums de discussão sobre os rumos para disseminação e uso destes ambientes. Alguns deles serão descritos a seguir.

2.3.1 **GGF, OGSA e OGSI**

O Global Grid Forum (GGF) é um comitê formado por representantes da indústria e da pesquisa ligados a tecnologia de grade. Este fórum tem fomentado a criação de documentos para padronização dos sistemas de grade. Documentos podem ser submetidos para este fórum para discussão e publicação. O seu funcionamento é semelhante ao sistema de RFCs do IETF (IETF, 2004).

Duas especificações merecem destaque no contexto no GGF: *Open Grid Services Architecture* (OGSA) e o *Open Grid Services Infrastructure* (OGSI). O OGSA (FOSTER et al, 2004) tem como objetivo definir conceitualmente os componentes de uma infra-estrutura de grade. Sua principal atribuição é identificar os serviços essenciais para grades, definindo o seu escopo e as suas inter-relações. O OGSI (TUECKE et al, 2003) é a descrição concreta dos mecanismos especificados no OGSA. Concebido sobre as novas tendências de processamento distribuído e *E-Business*, esse documento define o conceito de *Grid Service*, que é um *Web Service* especializado para aplicações de grade. *Web Services* possibilitam que aplicações diferentes se comuniquem, independentemente da linguagem ou ambiente sob o qual foram construídos. A grande extensão presente nos *Grid Services* em relação aos W*eb Services* é o controle de estado. *Web Services* não mantêm dados entre uma invocação e outra; *Grid Services*, sim.

Deve-se ressaltar a importância do GGF, do OGSA e do OGSI como fundamental para a ampla popularização e padronização das tecnologias de grade. É bem adequado citar Foster (2002) que nos remete a esta de idéia de forma muito direta: “No futuro, para que instituições façam parte de grades precisarão implementar os protocolos OGSA, tal como para fazer parte da Internet hoje uma entidade precisa ‘falar’ IP”. Uma vez que o OGSA baseia-se em serviços Web, ele incorpora especificações definidas em outras organizações de padronização como o W3C, IETF e OASIS, entre outras.

2.3.2 **EGA**

A Enterprise Grid Alliance (EGA) é uma organização aberta, neutra e sem fins lucrativos que busca desenvolver soluções e acelerar a distribuição de aplicações de computação em grade no mercado corporativo. Através de seus participantes, a EGA cria

recomendações para o melhor uso da tecnologia de computação em grade, com foco em modelos de referência, abastecimento, segurança e contabilidade. Com base em dificuldades encontradas por estas organizações, a meta é desenvolver soluções interoperáveis e um manual de boas práticas a ser adotado nas empresas para melhores resultados no uso desta tecnologia, com reflexo direto nos negócios de cada organização, melhor performance dos níveis de serviço e menor custos operacionais de TI.

Entre os participantes do EGA estão a Sun Microsystems, NEC, Fujitsu/Siemens, Intel, AMD, Hewlett-Packard, Oracle, Novell, Unisys, Cisco e Dell Computers, entre outros grandes fabricantes.

2.3.3 **OASIS**

OASIS (Organization for the Advancement of Structured Information Standards) é um consórcio internacional sem fins lucrativos que busca o desenvolvimento, convergência e adoção de padrões *e-business*. O consórcio cria mais padrões de serviços Web do que qualquer outra organização envolvida com padrões de segurança, e-business, esforços de padronização no setor público e para aplicações específicas do mercado. Fundada em 1993, a OASIS tem mais de cinco mil participantes (que representam mais de seiscentas organizações e membros individuais) em mais de 100 países.

2.3.4 **DMTF**

O DMTF (Distributed Management Task Force), fundado em 1992, é uma organização das Indústrias no sentido de guiar o desenvolvimento, adoção e interoperabilidade do gerenciamento de padrões e iniciativas para ambientes desktop, corporativos e Internet. Seu trabalho envolve os principais fabricantes e grupos de padronizações, disponibilizando um

gerenciamento mais integrado e de melhor custo através de soluções interoperáveis. Em geral, o uso dos padrões da DMTF reduzem os custos operacionais.

Com mais de três mil participantes de cerca de 200 organizações, o DMTF reune esforços de forma colaborativa em grupos de trabalho que buscam especificações e padrões. Entre seus membros principais, podemos citar a Cisco Systems, Dell Computer Corp., EMC, HP, Hitachi, IBM, Intel, Microsoft, Novell, Oracle, Sun Microsystems e Symantec, entre outros.

O DMTF também trabalha em parceria com muitas outras organizações como a OASIS (Organization for the Advancement Of Structured Information Standards), entre outras, e já formalizou oficialmente alianças com a EGA (Entreprise Grid Alliance) e o GGF (Global Grid Forum). Com o GGF, o DMTF busca unificar o abastecimento, compartilhamento e gerência de recursos e tecnologia de computação em grade. Enquanto o DMTF contribui com seu *expertise* em infra-estrutura de gerência distribuída e modelagem de recursos, o GGF contribui com extensões e requisitos para suporte de computação em grade, compartilhamento de recursos e abastecimento.

A parceria com a EGA busca fazer com que o *Commom Information Model* (CIM) do DMTF continue atendendo as necessidades da computação em grade, enquanto os requisitos de abastecimento específicos para ambientes de computação em grade sigam complementando o trabalho realizado pelo DMTF. Esta colaboração permite que os usuários modelem ambientes de Grid a partir do CIM do DMTF, provendo maior confidencialidade e segurança ao abastecimento e contabilidade nos ambientes de Grid propostos pelo EGA.

2.4 DESAFIOS DA SEGURANÇA

Devido à natureza extremamente distribuída e heterogênea a que a computação em grade se propõe, prover um ambiente seguro de execução é uma questão bastante desafiadora. Para a execução de uma tarefa em grade é interessante realizar algumas reflexões nesta ótica:

1. Como uma máquina que pertence à grade poderá decidir se deve executar a tarefa solicitada ou não ?

2. Como o processador que recebeu uma solicitação poderá se certificar que o solicitante da tarefa realmente é quem diz ser ?

3. Como o solicitante poderá garantir que a resposta enviada pelo processador que executou a tarefa é válida? Ou seja, como garantir que a máquina realmente executou a operação solicitada e não simplesmente enviou qualquer resultado ?

4. Como garantir que os pacotes não foram alterados na rede, antes de chegar ao seu destino (seja ao requisitante ou à máquina de grade) ?

5. Como o administrador poderá garantir que as suas máquinas que pertencem à grade não serão exploradas por tarefas maliciosas submetidas no contexto da grade ?

Na medida em que a computação em grade se destina a possibilitar a execução de aplicações em muitos domínios administrativos, estas e outras questões são bastante pertinentes. É certo afirmar que algumas destas questões já possuem respostas consensuais como, por exemplo, a questão 2, onde claramente uma alternativa seria a utilização de certificados digitais. Em contrapartida, verifica-se que várias ferramentas de computação em grade possuem modelos incompletos de segurança ou até mesmo inexistentes.

Um dos requisitos mais críticos a serem tratados é o estabelecimento de relações de confiança (*trusts*) entre os membros de uma organização virtua1. Tais organizações poderão ter as mais variadas naturezas, podendo ser criadas por um longo período (como em projetos

interinstitucionais de cooperação científica), ou mesmo para a execução de uma única tarefa. Assim, o overhead associado ao gerenciamento das relações de confiança precisa ser baixo (WELCH et al, 2003). Um outro agravante refere-se à estrutura extremamente dinâmica das organizações virtuais, nas quais novos recursos podem ser instanciados a qualquer momento. Essa dinâmica na adição de recursos à grade também precisa ser controlada, de forma a garantir que somente os elementos autorizados participem da organização virtual e tenham acesso aos seus serviços.

Requisitos de segurança em um ambiente de grade são regidos pela necessidade de suportar Organizações Virtuais escaláveis, dinâmicas e distribuídas (FOSTER, I. et al). De uma perspectiva de segurança, um atributo chave das VOs é que seus participantes e recursos sejam regidos pelas regras e políticas de suas organizações de origem. Além disso, enquanto algumas VOs, como as de colaboração científica, podem ser muito grandes e de vida longa, outras podem ser de curta duração, criadas apenas para suportar uma única tarefa, por exemplo. Um requisito fundamental é disponibilizar acesso à VO para recursos que existam em uma organização real e que, da perspectiva desta organização, tenha políticas que façam referência apenas aos usuários locais. Este acesso à VO deve ser estabelecido e coordenado apenas através de relações de confiança que existam entre o usuário local e sua organização e a VO e o usuário. Não se pode assumir relações de confiança entre organizações reais e a VO ou seus membros externos. Os mecanismos de segurança em grade apontam estes desafios, permitindo que uma VO seja tratada de forma que múltiplos recursos ou organizações "terceirizem" algumas políticas de controle para ela, a VO, que coordenará estas regras "terceirizadas" de uma forma consistente a permitir um uso coordenado dos recursos compartilhados.

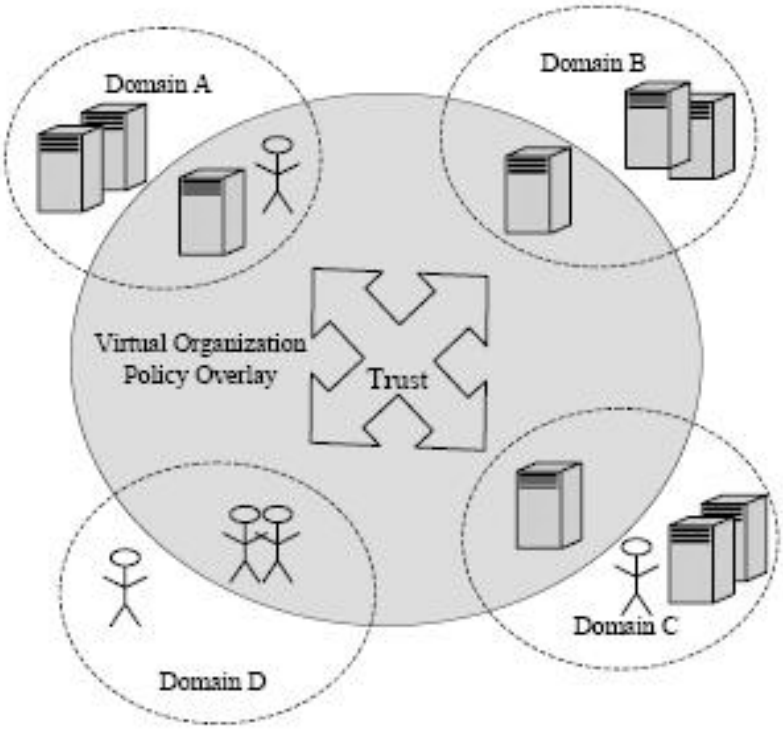

Figura 1 – Domínio de políticas de uma VO unindo participantes de diferentes domínios em um único e confiável domínio.

2.5 REQUISITOS DE SEGURANÇA

Para a execução segura de aplicações em sistemas distribuídos é necessário que as plataformas de grade realizem o tratamento dos requisitos de segurança inerentes a essa classe de aplicações. Conforme Sotomayor (2004), a comunicação segura é sustentada por três pilares principais: confidencialidade, integridade e autenticação. Na computação em grade, além destes, vários outros requisitos são considerados, (NAGARATNAMET al. 2004). Estes requisitos serão caracterizados a seguir.

2.5.1 **Autenticação**

A autenticação tem por objetivo assegurar que o remetente da mensagem é de fato quem afirma ser. A importância deste requisito pode ser verificada em duas situações: (1) no estabelecimento da comunicação entre entidades este requisito garante a autenticidade das mesmas; (2) na garantia de que em uma conexão realizada, uma terceira entidade não possa se fazer passar por uma das partes envolvidas com o propósito de envio ou recebimento não autorizado de mensagens.

Um fator complicador à garantia deste requisito em um ambiente de grade é a premissa do *single sign-on* (FOSTER, I. et al, 1998). Ou seja, um usuário ao executar uma aplicação na grade, deverá autenticar-se apenas uma vez. É importante relembrar que uma grade pode ser formada por várias instituições que normalmente não compartilham a mesma base de usuários. Neste cenário, como garantir que a credencial fornecida pelo usuário seja válida nos diferentes domínios administrativos ? A solução para este problema pode ser alcançada com a técnica de delegação de credenciais (BERMAN et al, 2003; WELCH et al. 2003; FOSTER et al. 1998), onde o usuário, após autenticar-se, fornece ao *middleware* o poder para agir em seu nome.

2.5.2 **Autorização**

Um serviço de autorização (ou de controle de acesso) para computação em grade deve ser capaz de restringir o acesso aos recursos baseando-se nas informações do requisitante, do recurso a ser acessado e dos detalhes da requisição (WELCH et al. 2003). Neste sentido, políticas de autorização devem ser suportadas, de forma a fornecer aos administradores a possibilidade de definir critérios de acesso aos recursos pelos quais são responsáveis. Atualmente, pode-se considerar três técnicas principais para a implementação

de autorização: *Access Control List* (ACL), *Capabilities* e *Role Based Access Control* (RBAC).

A técnica ACL se baseia na utilização de uma lista associada a cada recurso ou objeto, na qual são descritas as ações permitidas e quais entidades podem realizá-las. Uma operação só é permitida se o par entidade/operação está presente na ACL do objeto. Este é o modelo normalmente utilizado em permissões de sistemas de arquivos.

Em *Capabilities* a entidade responsável pelo recurso envia referências dos serviços disponíveis às entidades que podem acessá-los. Tais referências podem ser consideradas tickets, que são verificados a cada tentativa de acesso. O uso deste artifício pressupõe o emprego de um mecanismo para verificação da validade das referências, como, por exemplo, assinaturas digitais.

No RBAC, permissões estão associadas a papéis (roles), e usuários são definidos como membros dos papéis apropriados. Papéis estão próximos ao conceito de grupos, entretanto, um papel agrupa um conjunto de permissões e um conjunto de usuários, ao passo que um grupo é apenas um conjunto de usuários. Segundo (SANDHU et al, 1996) e (RIGHI et al, 2004), este modelo apresenta administração de permissões simplificada se comparado com outros mecanismos de controle de acesso.

2.5.3 **Confidencialidade**

Confidencialidade é o aspecto que garante que somente as partes envolvidas na comunicação serão capazes de processar as mensagens trafegadas. Normalmente, esta garantia está ligada à utilização de algum mecanismo de criptografia. Certas aplicações de grade necessitam de garantias de confidencialidade, pelos mesmos motivos que as aplicações

tradicionais, por exemplo, por estarem manipulando informações sensíveis e que não podem ser interceptadas por terceiros. Assim, as infra-estruturas de grade devem ser capazes de prover os mecanismos para proteger a comunicação entre os seus componentes.

2.5.4 **Integridade**

Um serviço de integridade garante que as mensagens são recebidas da mesma forma como foram enviadas. Na prática, qualquer alteração efetuada nas mensagens poderá ser detectada pelos participantes da comunicação. Da mesma forma que a confidencialidade, algumas aplicações de grade necessitam deste tipo de garantia. A integridade pode ser implementada com a adição de redundância às mensagens enviadas, como por exemplo, a partir de digests, segundo Veríssimo e Rodrigues (2000). Assim, o receptor poderá comparar a mensagem com os controles enviados, de forma a se certificar de que a mensagem não sofreu alteração após ter sido enviada.

2.5.5 **Não repúdio**

Esta propriedade garante que uma operação não possa ser negada pelo seu executor, seja o envio ou o recebimento de determinada mensagem. O principal uso deste aspecto está relacionado a transações financeiras, onde uma determinada entidade poderia obter vantagens na alegação de não envio e/ou recebimento de determinada mensagem. Na computação em grade, este requisito poderia ser garantido por um serviço seguro de logs (NAGARATNAM et al. 2004).

2.5.6 **Auditoria**

Entende-se por auditoria o ato de analisar o funcionamento de um sistema ou rede, no intuito de diagnosticar falhas, sejam elas intencionais ou não. Normalmente este requisito é implementado a partir de mecanismos de log. Através da análise de logs é possível verificar

as ações executadas em determinado serviço, bem como verificar o funcionamento de mecanismos de segurança, como autenticação, autorização e integridade, desde que estes estejam integrados ao serviço de log. Num ambiente de grade, o mecanismo de auditoria pode auxiliar na localização de nodos “maliciosos” ou na detecção de problemas técnicos.

2.5.7 **Reputação**

O mecanismo de reputação se baseia em determinados critérios para estabelecer graus de confiança às entidades envolvidas em uma comunicação. Com isso, é possível determinar o “risco” na utilização ou prestação de um serviço baseando-se na reputação de outra parte envolvida.

Em um ambiente de grade, este mecanismo pode ser empregado para verificar a credibilidade de determinada organização ou usuário. Por exemplo, a garantia de qualidade no processamento de um resultado pode ser assegurada pela reputação do participante. Em outro cenário, a reputação poderia ser empregada para dar maior prioridade de execução a entidades que mais contribuem com os outros participantes, executando as tarefas solicitadas.

Os requisitos de segurança discutidos nos itens acima deverão ser implementados como serviços para a sua utilização em grades de computadores. Segundo (NAGARATNAM et al, 2004), tais serviços devem ser instanciados independentemente entre si. Por exemplo, uma determinada aplicação poderá necessitar apenas de garantias de autenticação e outra necessitar de garantias de integridade e confidencialidade. Neste sentido, a primeira aplicação só deverá instanciar o serviço de autenticação, e a segunda, os serviços de integridade e confidencialidade.

Outra característica importante a tais serviços é a capacidade de serem descobertos. Uma aplicação que possui determinadas garantias de segurança deve publicar os requisitos necessários ao seu acesso. Suponha-se uma aplicação com necessidades de autenticação. O processador que a hospeda deverá informar esta necessidade para que os requisitantes, ao se conectarem, possam tomar conhecimento das mesmas e enviar as credenciais necessárias.

3 **METODOLOGIA DE PESQUISA**

3.1 INTRODUÇÃO

Este capítulo, aborda a metodologia de pesquisa que será usada neste projeto. Serão descritas as questões envolvidas, o tipo de pesquisa a ser seguido e o modelo de referência que dá sustentação às proposições apresentadas. Aqui estará exposto também o universo a ser investigado. As fases de coleta e análise de dados serão detalhadas e serão observadas algumas limitações que poderão ocorrer neste projeto.

3.2 QUESTÕES DA PESQUISA

O tema que norteia esta pesquisa são os aspectos de segurança em computação em grade. Como discutimos com bastante embasamento teórico no Capítulo 2, ao mesmo tempo em que a computação em grade vem ganhando o interesse de várias vertentes, tanto na área de pesquisa como uma verdadeira oportunidade de negócios, as questões sobre implementação de segurança ainda parecem causar desconfiança em alguns setores, impedindo uma maior popularização desta tecnologia. Podemos resumir a questão deste projeto de pesquisa com a seguinte pergunta:

Quais são os aspectos de segurança envolvidos atualmente em computação em grade e o que é projetado para a garantia de uma maior confiabilidade e a conseqüente maior utilização desta tecnologia no futuro ?

3.3 TIPO DE PESQUISA

Creswell (1994) elenca os dois principais paradigmas de pesquisa como sendo qualitativo e quantitativo. O paradigma de pesquisa aqui utilizado será o qualitativo. Pelo fato de ser uma tecnologia ainda em processo de amadurecimento no mercado, toda a discussão

sobre o que tem sido observado neste período podem gerar frutos extremamente positivos para um novo olhar a respeito do assunto e provocar linhas de pensamento para o futuro.

Com base em Vergara (1997), esta pesquisa é classificada exploratória, por analisar o fenômeno nos mercados científico-acadêmico e corporativo. Também descritiva e explicativa, pois estarão sendo expostas as características atuais da tecnologia no ambiente atual, estabelecendo relações de causa-efeito (principalmente pelo uso ou não de computação em grade devido à algum tipo de falta de segurança), o que poderá contribuir no entendimento sobre alguns dos fatores relacionados com o acontecimento do fenômeno.

Vergara (1997) ainda classifica uma pesquisa como sendo de campo (*survey*), de laboratório, telematizada, documental, experimental, *ex post facto*, participante, pesquisa-ação ou ainda estudo de caso. A pesquisa em questão será norteada como um Estudo de Caso, onde, mesmo que não haja um controle por parte do autor, ela torna-se atual e seus resultados podem ser bastante relevantes mesmo que não possam ser generalizadas. O Estudo de Caso tem caráter de profundidade e detalhamento. Baseia-se em poucas unidades de investigação. (VERGARA, 1997; ALVES 2003).

4 **ESTUDO DE CASO**

4.1 FERRAMENTAS

Atualmente, existem várias ferramentas para o desenvolvimento de grades, cada qual com as suas especificidades. Para ilustrar este referencial, serão apresentadas algumas ferramentas que são significativas no cenário atual.

- **Globus** (atualmente o padrão de fato entre as infra-estruturas para a criação de grades computacionais;
- **MyGrid/OurGrid**;
- **Condor**;
- **Sun Grid Engine**, (Sun Microsystems);
- **IBM Grid Tool Box** (IBM).

4.1.1 **Globus Toolkit**

A pesquisa em computação em grade produziu soluções de segurança baseadas não numa relação direta entre as organizações, mas no uso de uma "Organização Virtual" (VO) como uma ponte entre as entidades participantes em uma comunidade (WELCH et all). Os resultados desta pesquisa vem sendo incorporados de maneira intensa no Globus Toolkit, software desenvolvido pela Globus Alliance (entidade formada por universidades e centros de pesquisa dos Estados Unidos e da Europa) e largamente utilizado no cenário atual, que usa tecnologia de chave pública para endereçar solicitações de autenticação única (single sign-on), delegação e mapeamento de identificação, além de suporte à APIs padronizadas. A partir da versão 3.0, os serviços do Globus são definidos como *Grid Services*, em conformidade às especificações OGSA/OGSI. Os principais serviços presentes nesta infra-estrutura são: *Globus Resource Allocation Manager* (GRAM), *Monitoring and Discovery Service* (MDS), *Reliable File Transfer* (RFT) e *Grid Security Infrastructure* (GSI).

O GRAM é responsável pela alocação de recursos e gerenciamento de tarefas (Jobs). Fornece uma interface única que permite submeter, monitorar e controlar tarefas de forma independente do escalonador de recursos. O MDS fornece suporte a informações e sistema de diretórios. É formado por dois componentes principais, conforme (CZAJKOWSKI et al, 2001): *Grid Resource Information* (GRIS) e *Grid Index Information Service* (GIIS). O GRIS é um provedor configurável de informações sobre recursos implementado em LDAP. Já o GIIS é um *framework* para a construção de diretórios customizados. O RFT é o serviço responsável pela transferência segura de arquivos entre as máquinas da grade. O GSI é exatamente o nome dado à porção do Globus Toolkit que implementa a funcionalidade de segurança. O GSI provê mecanismos para autenticação e comunicação segura baseados em certificados X.509, infra-estrutura de chave pública (PKI), protocolos SSL/TLS e certificados proxy X.509 (WELCH et al, 2003). Em particular, a integração com serviços web e tecnologias de hospedagem de ambientes cria oportunidades para alavancar novas tecnologias e padrões de segurança como o XACML (*eXtensible Access Control Markup Language*) e o SAML (*Security Assertion Markup Language).*

Os serviços do Globus são oferecidos de forma independente, o que é considerado um fator importante para a sua ampla aceitação, de acordo com Cirne (2003). Essa possibilidade de utilização parcial do Globus fornece o suporte necessário para a migração gradual de aplicações paralelas para a sua utilização em grade. Entretanto, o fato de o Globus estar estruturado sob a forma de serviços independentes faz com que o mesmo não possa ser considerado uma solução pronta. Ou seja, é necessário certo esforço por parte de desenvolvedores e administradores para a utilização desta infra-estrutura de grade. Segundo Cirne (2003), muitas vezes é necessário desenvolver escalonadores de aplicação para o Globus, pois eles devem ser especializados às aplicações a serem executadas e levar em consideração a topologia existente.

O enfoque do Globus é muito abrangente, podendo ser aplicável a qualquer cenário de grade. Enquanto outras ferramentas são focadas em determinado tipo de aplicações, o Globus é flexível para ser empregado em qualquer situação, mesmo que isto despenda um esforço maior de implementação.

4.1.1.1 Grid Security Infrastructure (GSI)

O GSI usa criptografia de chave pública (também conhecida como criptografia assimétrica) como base para sua funcionalidade. Muitos dos termos e conceitos usados nesta descrição do GSI vem do uso do mecanismo de criptografia de chave pública.

As principais motivações para o GSI são:

- A necessidade de comunicação segura (autenticada e confidencial) entre elementos de um Grid Computacional;
- A necessidade de prover segurança através dos limites de uma organização, impedindo, desta forma, um sistema de segurança centralizado;
- A necessidade de suportar o "single sign-on" para usuários do Grid, incluindo delegação de credenciais para jobs computacionais que envolvem múltiplos recursos e/ou sites.

4.1.1.1.1 **Certificados**

O conceito central na autenticação do GSI é o certificado. Cada usuário e serviço no Grid é identificado através de seu certificado, o qual contém informações fundamentais para sua identificação e autenticação nos serviços que deseja utilizar.

O certificado do GSI inclui quatro itens principais de informação:

- Um nome (sujeito), que identifica a pessoa ou objeto que o certificado representa;

- A chave pública pertencente à este sujeito;
- A identidade da Autoridade Certificadora (CA) que assinou o certificado para validar que a chave pública e a identidade pertencem realmente ao sujeito em questão;
- A assinatura digital da CA.

É importante notar que a terceira parte envolvida (a CA) é usada para certificar a relação entre a chave pública utilizada e o sujeito no certificado. Com o intuito de confiar no certificado e em seu conteúdo, os certificados de uma CA deve ser confiável. A relação entre a CA e seu certificado deve ser estabelecido através de algum meio não criptográfico, senão o sistema não é confiável.

Os certificados do GSI são codificados no formato X.509, um padrão de formato de dados para certificados estabelecido pelo Internet Engineering Task Force (IETF). Estes certificados podem ser compartilhados com outros softwares baseados em chave pública, incluindo Navegadores (Browsers) da Microsoft ou Netscape.

4.1.1.1.2 **Autenticação Mútua**

Se duas partes tem certificados e se ambas confiam nas Autoridades Certficadoras que assinaram cada um dos certificados, então as duas partes podem provar para a outra que elas são quem dizem que são. Isto é conhecido como autenticação mútua. O GSI usa o protocolo SSL (Secure Socket Layer) para sua autenticação mútua. O SSL também é conhecido por um novo nome padronizado pelo IETF: TLS ou Transport Layer Security.

Antes da autenticação mútua ocorrer, as partes envolvidas devem primeiro confiar nas CAs que assinaram cada um dos certificados. Na prática, isto significa que elas deverão

ter cópias dos certificados das CAs, que contém as chaves públicas das CAs, e devem confiar que estes certificados realmente pertencem às Autoridades Certificadoras. Para se autenticarem mutuamente, o computador A estabelece uma conexão com o computador B. Para iniciar o processo de autenticação, A dá à B seu certificado. Este certificado diz à B quem A está dizendo ser, qual é a chave pública de A e qual Autoridade Certificadora está sendo usada para validar o certificado. O computador B primeiramente terá certeza que o certificado é válido conferindo a assinatura digital da CA. Isto dará à B a certeza que a CA realmente assinou o certificado e que ele não foi alterado. Neste ponto é onde B deve confiar na CA que assinou o certificado do computador A.

Uma vez que B confirmou o certificado de A, B deve ter certeza que A realmente é a pessoa identificada no certificado. B , então, gera uma mensagem aleatória (técnica do "*challenge-response"*) e a envia para A, pedindo à A que a criptografe. O computador A criptografa a mensagem usando sua chave privada e a devolve para B. B descriptografa a mensagem usando a chave pública de A. Se o resultado for a mensagem original enviada por B, então B sabe que A é quem ele diz ser.

Agora que B confia na identidade de A, a mesma operação deve ocorrer no modo inverso. B envia seu certificado para o computador A. A valida o certificado e envia uma mensagem (challenge) para ser criptografada por B. O computador B criptografa a mensagem e a devolve para A (response), A descriptografa a resposta e compara com a mensagem original. Se elas são iguais, então A tem certeza que B é quem ele diz ser.

Neste ponto A e B estabeleceram um conexão confiável, na qual cada um tem certeza acerca da indentidade do outro.

4.1.1.1.3 **Comunicação Confidencial**

Por padrão, o GSI não estabelece comunicação criptografada entre as partes envolvidas. Uma vez que a autenticação mútua é realizada, o GSI não interfere mais na comunicação, e ela poderá ocorrer sem o "overhead" de constantes encriptações/decriptações. Porém, o GSI pode ser facilmente usado para estabelecer um compartilhamento de chaves para encriptação se a comunicação confidencial é algo necessário. As leis americanas, sempre muito duras quanto à troca de mensagens criptografadas, já permite que o GSI tenha, como opcional, esta comunicação criptografada entre as partes envolvidas de um Grid Computacional. Desta forma, a confidencialidade pode ser aplicada.

Em relação à integridade dos dados, ela é padrão na comunicação do GSI. Mesmo que alguém leia o conteúdo da mensagem compartilhada entre duas partes de um Grid (sem a aplicação de confidencialidade), ele não poderá alterá-la em nenhum dos sentidos. Há também a opção de desativar este recurso caso seja o desejo do usuário.A integridade inclui também algum "overhead" na comunicação, porém bem inferior que o da confidencialidade (criptografia).

4.1.1.1.4 **Provendo segurança às chaves públicas**

O núcleo do software do GSI fornecido pelo Globus Toolkit sabe que a chave privada do usuário pode estar armazenada em um arquivo no computador local, uma vez que nem todos usam tokens ou smart cards. Para prevenir que outros usuários do mesmo computador tenham acesso à esta chave privada, o arquivo que a contém é criptografado com uma senha. Para usar o GSI, o usuário deverá entra com a senha solicitada para descriptografar o arquivo que contém a chave privada. O GSI, como citado anteriormente, suporta o uso de Tokens e Smart Cards para armazenamento das chaves privadas de seus usuários.

4.1.1.1.5 **Delegação e "Single Sign-On"**

O GSI prove uma capacidade de delegação, uma extensão do protocolo SSL que reduz o número de vezes que um usuário deve entrar com sua senha. Se um Grid Computacional necessita de muitos recursos de Grid sejam usados (que irão requerer autenticação mútua), ou se há necessidade de se ter agentes (locais ou remotos) solicitando serviços de interesse do usuário, a necessidade do usuário entrar várias vezes com sua senha pode ser evitada com a criação de um Proxy.

Um Proxy consiste de um novo certificado (com uma nova chave pública) e uma nova chave privada. O novo certificado contém a identidade de seu proprietário, modificada ligeiramente para indicar que este é um Proxy. O novo certificado é assinado pelo seu proprietário em vez da Autoridade Certificadora (veja a Figura 2). O certificado também inclui um campo de tempo, após o qual o Proxy não poderá mais ser aceito por outras solicitações. Um Proxy tem tempo de vida limitado.

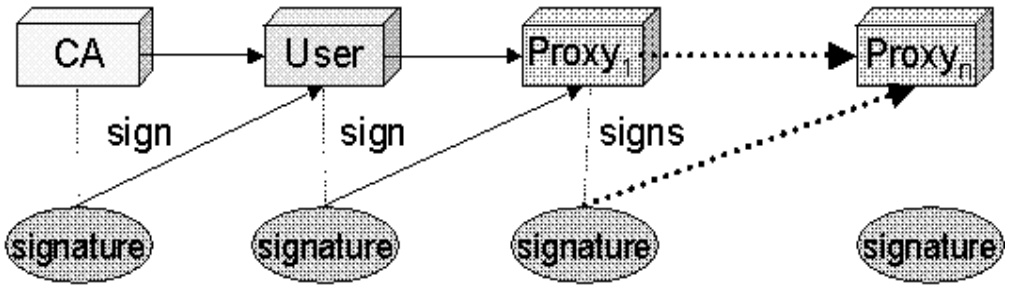

Figura 2 – Diagrama de autenticação via Proxy

A chave privada do Proxy deve ser mantida segura, porém, uma vez que ele tem um tempo de vida determinado, ela não precisa estar tão segura quanto a chave privada do usuário (que pode usar Tokens ou Smart Cards). Uma vez que um Proxy é criado, o usuário poderá

usar o certificado e a chave privada do Proxy para para autenticação mútua sem a necessidade de entrar com sua senha. Quando os Proxies são usados, o processo de autenticação mútua muda um pouco. A parte remota recebe não apenas o certificado do Proxy, mas também o certificado de seu proprietário. Durante a autenticação mútua, a chave pública do proprietário (obtida a partir de seu certificado) é usada para validar a assinatura no certificado do Proxy. A chave pública da Autoridade Certificadora é então usada para validar a assinatura no certificado do proprietário. Isto permite estabelecer uma rede de confiança a partir da Autoridade Certificadora para o Proxy, através do seu proprietário.

É importante perceber que os softwares baseados no GSI são os únicos que suportam as extensões de delegação para TLS (ou SSL). O projeto do Globus trabalha exaustivamente com o Grid Forum e o IETF para estabelecer os Proxies como uma extensão padrão para TLS, permitindo, então, que os Proxies GSI possam ser usados com outros softwares TLS.

4.1.2 **MyGrid e OurGrid**

MyGrid é uma ferramenta de suporte à implementação de grades computacionais, desenvolvida pela Universidade Federal da Campina Grande. Esta ferramenta foi concebida com o objetivo de se tornar uma solução simples e completa. Simples, neste contexto, enfatiza o fato de que o MyGrid foi projetado para se aproximar o máximo possível de uma solução *out-of-the-box*, que possa ser utilizada com o mínimo de esforço, escondendo do usuário os detalhes de implementação da grade. O fato do MyGrid objetivar ser uma solução completa menciona que ele deve cobrir todo o ciclo de produção de uma solução de grade, do desenvolvimento à execução, abrangendo também a manipulação dos parâmetros de entrada e dos resultados. Porém, para atingir esses objetivos esta ferramenta não suporta aplicações de grade genéricas, sendo orientado somente a aplicações do tipo *Bag-of-Tasks* (BoT). *Bag-of-Tasks* são aplicações paralelas, cujas tarefas são independentes, podendo, assim, ser

executadas em qualquer ordem. Pela natureza fracamente acoplada deste tipo de aplicação, BoT podem potencialmente usar um número muito grande de processadores.

Além do *middleware*, esta ferramenta oferece as abstrações e os serviços necessários para a criação e uso da grade. Se comparado a outras ferramentas, o MyGrid implementa um conjunto simplificado de serviços: execução remota e transferência de arquivos. Uma outra simplificação na arquitetura MyGrid é a formação da grade. Para o MyGrid, a grade de um determinado usuário é formada por todas as máquinas que ele pode acessar. Assim, uma grade de um usuário poderá ser formada pelas máquinas de sua instituição, de uma outra instituição na qual ele possui acesso, de algum provedor contratado para fornecer ciclos de processamento ou mesmo de algum amigo que forneceu uma conta para acesso a sua máquina.

No entanto, essa solução para acesso a outros domínios administrativos não é escalável, pois uma conta para o usuário deverá ser criada em cada domínio que ele necessitar acessar. Para contornar essa limitação, foi desenvolvido o projeto OurGrid, que visa a desenvolver tecnologias para a utilização em larga escala da computação em grade. O OurGrid estabelece uma rede peer-to-peer de sites que compartilham recursos com o objetivo de formar uma grade à qual todos tenham acesso. O ponto central do OurGrid é que o compartilhamento de recursos é feito usando o modelo de rede de favores..

Questões relativas à segurança têm sido postergadas nas grades MyGrid e OurGrid, possivelmente em função de prioridade na adição de funcionalidades às mesmas. Pode-se, inclusive, afirmar que a grade formada por essas duas ferramentas carece de um modelo de segurança. Alguns mecanismos para tratamento de segurança têm sido adicionados, como a utilização do protocolo SSH para comunicação entre os componentes da grade e transferência

de arquivos. Andrade (2004) propõe um método para assegurar a integridade na execução das tarefas baseado na replicação entre as mesmas. Porém, tais mecanismos são oferecidos de maneira isolada, sem integração ou mesmo preocupação em abranger todos os requisitos de segurança inerentes a essa classe de aplicações. Neste ambiente, vários tipos de ataques são possíveis de serem realizados, como *spoofing* (onde um *peer* malicioso pode facilmente enviar requisições para outros participantes); acesso desautorizado a qualquer recurso (devido à inexistência de um sistema de controle de acesso); e ainda, as mensagens podem sofrer alterações na rede após terem sido enviadas. Dessa forma, a criação de um modelo de segurança para essas duas grades é considerada um problema em aberto e de vital importância.

4.1.3 **Condor**

O Condor é uma ferramenta desenvolvida na Universidade norte-americana de Wisconsin Madison. Seu principal objetivo é fornecer grande poder computacional a médio e longo prazo, utilizando processadores ociosos na rede (LITZVKOW et al, 1988). Entenda-se disto que o Condor visa oferecer um desempenho sustentável a médio e longo prazo (dias a semanas), mesmo que o desempenho instantâneo do sistema possa variar consideravelmente (CIRNE, 2003). Esta ferramenta é especializada na execução de aplicações cujas tarefas são independentes, sendo considerada, portanto, uma ferramenta para a execução de aplicações *Bag-of-Tasks*.

O usuário submete à ferramenta as tarefas que devem ser executadas remotamente. O Condor localiza as máquinas ociosas na rede e envia a elas as tarefas para execução. Assim, o usuário tem a percepção de que as tarefas estão sendo executadas localmente. Neste cenário, nem sempre a máquina remota possui acesso ao mesmo sistema de arquivos utilizado na máquina do usuário. Assim, para resolver este tipo de situação, a máquina remota Condor faz

o redirecionamento das chamadas de sistema locais para a máquina onde a execução foi solicitada. Tal operação é realizada pela biblioteca de redirecionamento Condor (CIRNE, 2003).

O Condor foi inicialmente concebido para a execução em NOWs *(Network of Workstations*) (LITZVKOW et al, 1988). Uma NOW configurada para a execução do Condor é chamada de Condor Pool. Posteriormente o Condor foi adaptado para a implementação de grades. O fato de o Condor ser especializado em aplicações *Bag-of-Tasks* facilitou bastante esta adaptação.

4.1.4 **Sun Grid Engine**

O software Sun Grid Engine oferece um ambiente de recursos que visa maximizar a potência disponível da rede local aumentando a produtividade em ambiente de computação em grade. O software Sun Grid Engine é um modelo escalável de hardware, software e serviços para este tipo de tecnologia.

O software Sun Grid Engine (ferramenta de DRM da Sun) localiza os recursos inativos e os aproveita, com promessa de que uma organização possa obter até cinco vezes mais rendimento de seus sistemas em rede (segundo o fabricante). É oferecido “de acesso confiável, consistente”. Em um ambiente Sun Grid Engine, os trabalhos são mantidos em uma área central e as filas que fornecem os serviços para a execução dos trabalhos são associadas a sistemas de computação individuais. Os requisitos dos trabalhos podem ser bastante diferentes e apenas determinadas filas podem ser capazes de fornecer o serviço correspondente. Os requisitos especificados geralmente são memória disponível, velocidade de execução e licenças de software disponíveis.

A ferramenta corresponde aos recursos disponíveis aos requisitos dos trabalhos. Um usuário que envia um trabalho à ela especifica um perfil para ele. Ao mesmo tempo a identidade do usuário e a hora de envio também são armazenados. Assim que um recurso se torna disponível para execução de um novo trabalho, o software determina quais são os trabalhos adequados para o recurso e despacha o trabalho com a prioridade mais alta ou o tempo de espera mais longo. As filas do Sun Grid Engine permitem a execução de muitos trabalhos simultaneamente. O software Sun Grid Engine inicia novos trabalhos na fila que estiver menos carregada e for a mais adequada.

A Sun Microsystems deseja ver uma grande adoção de sua arquitetura para computação em grade. Para isto, já disponibilizou para download em seu site a os arquivos fontes e binários do Sun Grid Engine para instalação em Linux. A SuSE Linux já traz em sua distribuição uma versão Open Source (Código Aberto) da ferramenta. Esta versão é licenciada pela Sun Industry Standards Source License, porém não é permitido que alterações no código-fonte sejam compartilhadas por aqueles que implementam esta solução. O produto é livre para implementação em qualquer número de CPUs e é livre para uso para utilização em plataformas Linux (x86) e SPARC.

A visão da Sun para computação em grade se dá em três níveis. No primeiro nível estão os chamados *Clusters* locais, onde a ferramenta de Grid mantém uma lista de tarefas e uma lista de recursos capazes de realizá-la. Os recursos ficam ocupados até que a tarefa seja realizada. O segundo nível, chamado de *Campus* ou *Enterprise*, unifica grades para compartilhar seus recursos, quando há necessidade de maior poder computacional, por exemplo. No terceiro nível, chamado de *Global*, a filosofia é a mesma, porém estamos tratando de Redes geograficamente distantes, indo além das barreiras dos *Firewalls* de uma Instituição.

4.1.5 **IBM Grid Toolbox**

O IBM Grid Toolbox é uma ferramenta para criação e hospedagem de serviços de computação em grade. Este produto inclui, na realidade, material desenvolvido pela Globus Alliance, bem como um conjunto de APIs e ferramentas de desenvolvimento para a criação de aplicação e serviços de computação em grade. É capaz de executar serviços e aplicações de *Grid* e compartilhá-los com outros participantes (provedores e usuários). Sua variedade de ferramentas inclui gerência e administração de serviços de computação em grade, hospedagem de *Grid*, e um ambiente gráfico para administração, o *Grid Services Manager*.

Esta ferramenta tem seu uso limitado à sistemas operacionais Linux ou AIX rodando em Servidores IBM. Ela inclui um SDK (*Software Developers Kit*) que provê uma série de informações e ferramentas adicionais para desenvolvedores em computação em grade. Todos os serviços disponíveis no IBM Grid Toolbox são padronizados segundo a interface OGSI, a mesma usada no Globus Toolkit, o que facilita a interoperação desta ferramenta com outras de computação em grade baseadas no mesmo conceito, o que é um facilitador.

Quanto à segurança, o IBM Grid Toolbox usa o GSI, mesmo conceito usado no Globus Toolkit. Com ele é possível ter autenticação segura e comunicação sobre redes abertas. A base deste conceito está sustentada na política de Encriptação de chave pública (criptografia assimétrica), Certificados X.509 e aditivos para o GSS-API (*Generic Security Service API*), que é o padrão API para segurança em sistemas promovido pelo IETF. Com isso, busca-se a comunicação segura entre elementos de um Grid mesmo através de limites de suas redes e suporte à single sign-on (autenticação uma única vez) por parte de seus usuários.

4.2 REQUISITOS DE SEGURANÇA DO GGF

Na gestão de segurança em TI, gerenciar o risco é, em termos práticos, manter um equilíbrio entre vulnerabilidades e ameaças (Módulo Security Solutions, 2005). A partir do ponto de vista de um gerente de segurança, um ambiente de Grid representa um alvo em potencial para qualquer invasor. Em um abiente de computação em grade há muitos requisitos necessários para manter a sua segurança. A pergunta é: como a área de segurança do GGF lida com isso atualmente ?

Uma coisa é certa: o GGF não pode, simplesmente, limitar-se aos conceitos básicos de segurança. Há necessidade de um software suficientemente operacional, robusto e flexível, que trabalhe de forma a permitir todos os tipos de contingências e, além de tudo isso, fornecer segurança em todas as fases do grid. Um dos grandes problemas com a implementação de segurança baseada em infra-estrutura de chave pública (PKI) é a complexidade envolvida. Há chaves públicas e privadas e ambas precisam ser gerenciadas; há níveis hierárquicos de autoridades certificadoras; e há o processo de encriptação e decriptação da informação antes de ser efetivamente compartilhada. Apesar de toda sua complexidade, esta solução é bastante popular justamente pela confiabilidade agregada.

4.2.1 **Grupos de Trabalho e Pesquisa sobre segurança**

O GGF possui alguns grupos de trabalho envolvidos em pesquisas e implementações de segurança em ambientes de Grid. Abaixo estão listados alguns deles.

4.2.1.1 Authorization Frameworks and Mechanisms WG (AuthZ-WG)

A busca por mecanismos de autorização avançados, flexíveis e específicos norteia os trabalhos deste grupo, que busca definir *framework* conceitual de autorização em ambientes de Grid para os desenvolvedores de aplicações neste cenário. O objetivo principal é

categorizar os módulos e sistemas existentes para a área de autorização visando uma padronização. Outra importante tarefa deste grupo é colocar estes serviços e módulos em conformidade com as novas arquiteturas de Grid que estão em desenvolvimento, unindo esforços com o trabalho feito por outros grupos como o OGSA-Sec e o SA3.

4.2.1.2 Open Grid Services Architecture Security Working Group (OGSA-Sec)

O propósito deste grupo é enumerar e endereçar os requisitos de segurança no contexto da OGSA. Uma vez que a OGSA alavanca os serviços web, a arquitetura de segurança da OGSA irá alavancar os fundamentos de segurança nos serviços web, publicados nas especificações do WS-Security (Web Services Security Roadmap, publicado em abril de 2002). O OGSA-Sec irá monitorar de perto os esforços relacionados com outras comunidades (por exemplo, o OASIS), com a intenção de não haver duplicação de trabalho. O primeiro trabalho deste grupo foi o documento "*The Security Architecture for Open Grid Services*" . Ele descreve uma arquitetura que busca estar alinhada com o modelo de segurança definido pelo framework de serviços web da própria OGSA. O segundo trabalho foi o "OGSA *Security Roadmap*", que enumera um conjunto de especificações a serem definidas no GGF com o objetivo de garantir a interoperabilidade das implementações da arquitetura de segurança do OGSA.

4.2.1.3 Certificate Authority Operations Working Group (CAOPS-WG)

Seu propósito é desenvolver procedimentos operacionais e recomendações que facilitem o uso do certificado X.509 e outras tecnologias para autenticação entre ambientes de grid. Com o desenvolvimento de boas práticas, o grupo busca facilitar serviços mútuos de autenticação. O GGF tem desenvolvido um modelo de CP (*Certificate Policy*) / CPS (*Certification Practice Statement*) para seu usado por “sites” e organizações virtuais que desejam implementar uma autoridade certificadora. CP é o nome dado ao conjunto de regras

que indica a aplicabilidade de um certificado para uma comunidade particular. Já o CPS é a definição de práticas com a qual uma autoridade certificadora gera seus certificados. O CAOPS-WG foca exatamente nesta necessidade das autoridades certificadoras, sem trabalhar na gerência da chave privada de usuários.

4.2.1.4 OGSA Authorization Working Group (OGSA-AUTHZ)

Ele define as especificações necessárias a permitir a interoperabilidade básica e a associação de components de autorização no *framework* da OGSA. Devido ao grande número de sistemas de autorização para ambientes de Grid no cenário atual (Akenti, PERMIS, CAS, VOMS, Cardea, etc...), estas especificações permitem à estas soluções serem intercambiáveis através de um *middleware* que requeira a funcionalidade de autorização.

4.2.1.5 Site Authentication, Authorization, and Accounting Requirements RG (SA3-RG)

O objetivo da pesquisa deste grupo é coletar e codificar os requisitos dos ambientes de Grid existentes com relação à aceitação de credenciais para acesso aos seus serviços. Onde estes requisitos não são uniformes ou até mesmo exclusivos, o grupo recomendará que as aplicações existents possam prover para estes ambientes exclusivos uma maneira de inserir seus próprios conjuntos de requisitos.

4.2.1.6 Authority Recognition Research Group (ARRG-RG)

A relação de confiança entre entidades em muitas transações é disponibilizada por algum elemento de autoridade (por exemplo, certificado X.509 ou o ticket Kerberos) considerando sua identidade, alguma outra característica (os muitos dispositivos e elementos de autenticação) ou ambas.

As afirmações disponibilizadas por uma autoridade devem ser reconhecidas como válidas e apropriadas para este requisitos antes que uma das partes possa confiar nestas informações. Se uma afirmação de uma autoridade específica é apropriada ou não, isso dependerá de vários fatores, incluindo o comprometimento que a autoridade tem com a informação que afirma, as obrigações que assume em relação às partes ao fazer tal afirmação, etc... Muitas vezes, os mecanismos existentes não facilitam a disseminação desta informação pela autoridade.

O Authority Recognition Research Group tem por objetivo explorer o potencial de um mecanismo simples, barato, o mais automático possível, no qual uma das partes envolvidas na transação de confiança possa decidir por reconhecer (ou não) as afirmações feitas por uma autoridade. Espera-se que tais mecanismos sejam simples e forneçam o estabelecimento seguro e confiável entre participantes de um grid.

4.3 REQUISITOS DE SEGURANÇA DA EGA

Em julho de 2005, a Enterprise Grid Alliance publicou um documento no qual relaciona requisitos de segurança para aplicações de computação em grade. É uma recomendação, baseada nos resultados das discussões entre seus membros, visando informar aos usuários sobre riscos e ameaças inerentes aos serviços de computação em grade. O documento, que é resultado dos esforços do grupo de trabalho de "*Grid Security*", identifica ameaças e necessidades de segurança relacionadas com computação em grade e como elas podem ser minimizadas e atendidas. As empresas podem fazer uso destas informações para o melhor desenvolvimento de seus produtos ou a melhor configuração de seus sistemas, deixando-os mais seguros e competitivos. As aplicações corporativas podem ter componentes em tempo real ou "*batch*", podem ser geograficamente distribuídas e podem ser baseadas em softwares comerciais ou de código aberto.

A idéia inicial documento foi lançar mão do amplo conhecimento dos membros da EGA em termos de Computação em Grade e Segurança da Informação e identificar requisitos únicos de segurança para uma "Arquitetura Corporativa para Computação em Grade" para usuários finais, Organizações e fabricantes em geral. Toda a questão de Infra-estrutura computacional foi revista e os riscos e ameaças relativos à computação em grade foram identificados. O espírito colaborativo entre as organizações componentes do EGA propiciou a formulação de padrões que buscam minimizar redundâncias na área de desenvolvimento de aplicações e eliminam barreiras na adoção desta tecnologia.

Uma vez que os ambientes de computação em grade são uma evolução adaptada da computação corporativa, deve ser considerado que as políticas de segurança , requisitos e regulamentações referentes à computação corporativa também poderão ser aplicadas à computação em grade. É bastante vasto o material de recomendações acerca de segurança em redes de computadores, incluindo normas, padrões, organizações, etc... Os tópicos de segurança desta natureza, normalmente são baseados nos seguintes controles:

- "*Hardening*" de plataformas e aplicações. Entende-se por "Hardening" como sendo o processo de tornar um sistema seguro, especialmente visando a proteção contra ataques intencionais;
- Autenticação, controle de acesso e auditoria para plataformas e aplicações.
- Configuração, filtragem, monitoração e criptografia para segurança de redes de computadores.

Estes tópicos não são novos e vem sendo aplicados no mercado. O objetivo do modelo de referência da EGA é alavancar o trabalho já feito por várias entidades como base para recomendações de segurança específicas para ambientes de computação em grade.

4.3.1 **Modelo de referência de Segurança**

Um "Grid corporativo" (*enterprise grid*) é uma coleção de "**componentes de Grid"** (*Grid components*) sob o controle de uma "**entidade gerenciadora do Grid"** (*Grid management entity*). Grids corporativos também são diferenciados de *datacenters* tradicionais pelas práticas de gerenciamento e tecnologia, as quais disponibilizam mais gerenciamento de serviços ou aplicações do que gerenciamento de componentes, além de disponibilizarem também o "pooling" e o compartilhamento de recursos de rede. Não é objetivo deste documento entrar em maiores detalhes sobre o modelo de referência da EGA. Vamos, a seguir, discutir aspectos de segurança em arquiteturas corporativas de Grid propostos pela EGA.

4.3.1.1 Segurança dos componentes de Grid

Um componente de Grid é definido como uma classe de objeto do qual todos os outros componentes que são gerenciados em um Grid corporativo descendem. Isto inclui tudo o que é relativo à servidores, componentes de rede, "*arrays*" de discos para aplicações e serviços como base de dados, ERP, etc... A natureza dos componentes de Grid é que eles podem geralmente ser combinados em uma grande variedade de maneiras para formar os mais sofisticados elementos (sendo também, cada um deles, componentes de grid).

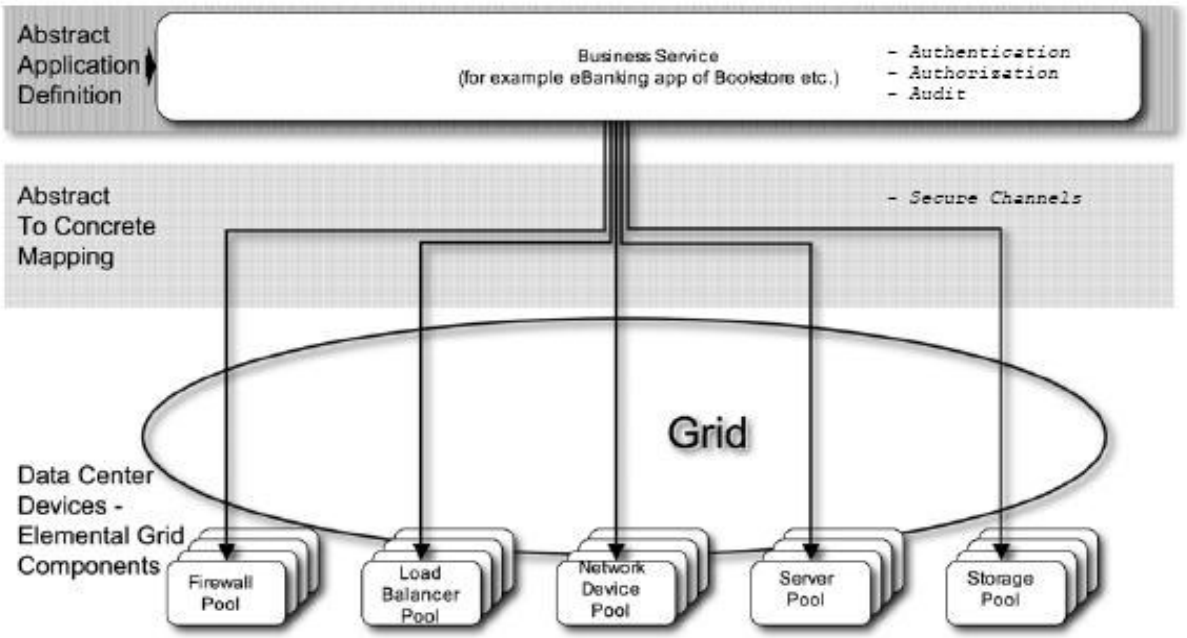

Figura 3 – Abstração do mapeamento de componentes de um Grid

A figura 3 ilustra um exemplo simples de um mapeamento de alto nível entre um serviço e seus componentes físicos e lógicos subjacentes. Deve ser compreendido que cada componente físico e lógico do Grid tem suas próprias características e controles de segurança. Isto não é, de fato, diferente do que produtos e componentes individuais são distribuídos atualmente. Cada um deve ser protegido ou estar combinado com outros componentes para receber nível de segurança e proteção desejados. Da mesma forma, a agregação e combinação de componentes de Grid podem também ter necessidades ou características de segurança únicos que são adicionais à união lógica dos próprios elementos. Mais uma vez, é importante lembrar que não há diferença de como estes componentes seriam distribuídos em data centers tradicionais nos dias de hoje. A Computação em grade corporativa não nega a necessidade de princípios de segurança tradicionais e todos os controles nas áreas de identificação, autenticação, autorização, confidencialidade, integridade, disponibilidade, não-repúdio e auditoria, entre outros. Se todos eles são necessários em uma

arquitetura corporativa tradicional, eles provavelmente também serão necessários em um ambiente corporativo de grid.

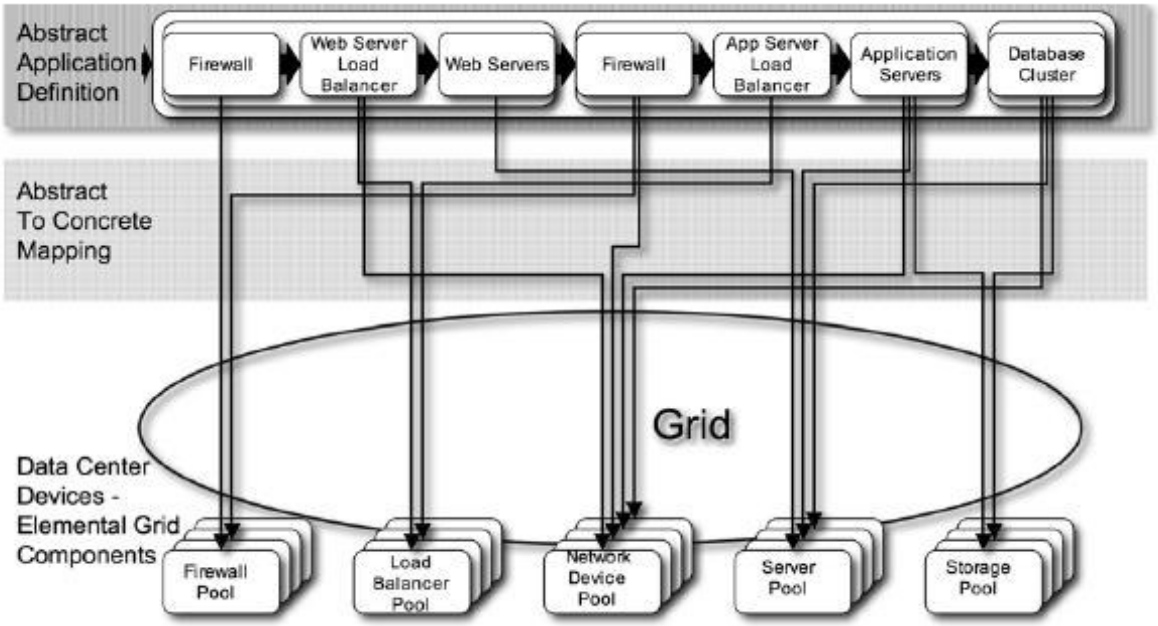

Figura 4 – Abstração do mapeamento de componentes de um Grid (2)

A Figura 4 acima mostra um exemplo que destaca como os componentes discretos que podem estar fisicamente separados podem agora ser mapeados para um "pool" compartilhado de componentes físicos de grid. Neste caso, há questões de segurança que, embora não sejam novas, são mais proeminentes em um ambiente de grid. Quando movidos de um ambiente físico isolado para um abiente onde os componentes são monitorados e compartilhados por muitas aplicações e serviços (nem sempre relacionados), os recursos monitorados precisam prover separação lógica e segurança entre as diferentes aplicações. Por exemplo, um recurso de armazenamento pode conter informações que devam ser apenas acessadas por uma única aplicação, mesmo se o "pool" de armazenamento atual seja usado por outras aplicações diferentes.

Esta variedade de separação lógica não é totalmente única para o ambiente corporativo de grid, mas é muito importante. Da mesma forma, o tráfego de rede precisa ser dividido de forma apropriada entre diferentes aplicações e serviços mesmo se eles estão executando em recursos compartilhados. Dependendo dos requisitos definidos por um serviço e nível de confiança e proteção requeridos, a separação física ou elétrica ainda pode ser solicitada para certos componentes. A arquitetura corporativa de Grid deve ser flexível o suficiente para, ainda assim, estender recursos dedicados através da definição de suas políticas de segurança, que irão facilitar a implementação de conceitos como o de privilégio mínimo e a defesa em camadas. Os conceitos de segurança relacionados à monitoração de recursos se aplicam tanto aos recursos lógicos como serviços compartilhados (diretórios, logs, etc...) quanto aos controles como mecanismos de cluster, filtro de pacotes, sistemas de detecção de intrusão (IDS), etc...

Os componentes de Grid tem características e atributos de seguranças associados à eles. Estes atributos podem ser internos ao componente do Grid (por exemplo, permissões de um arquivo em um sistema de arquivos) ou podem ser explicitamente associados com o componente de Grid gerenciado na entidade gerenciadora do grid. Além disso, os componentes podem definir dependências específicas. Tais dependências podem ser colocadas em atributos específicos para o componentes ou em elementos externos. Estas dependências ajudam a reforçar as políticas de segurança e assegurar que as vulnerabilidades são minimizadas.

Este conceito abrangente de dependências em grids corporativos permitiriam que serviços inteiros fossem provisionados, configurados e disponibilizados de forma segura. Cada passo nesta direção ajudariam a minimizar os riscos e limitar a exposição destes componentes. Porém vale lembra que estas possibilidades não estão imunes aos riscos. Atributos fracos ou

dependências desalinhadas podem abrir brechas no ambiente ou, ainda, causar indisponibilidade de serviços no grid.

4.3.1.2 Ciclo de vida de um componente de grid

O modelo de referência da EGA define os seguintes estados de ciclo de vida de um componente de grid: abastecimento, administração contínua e desativação / reaproveitamento.

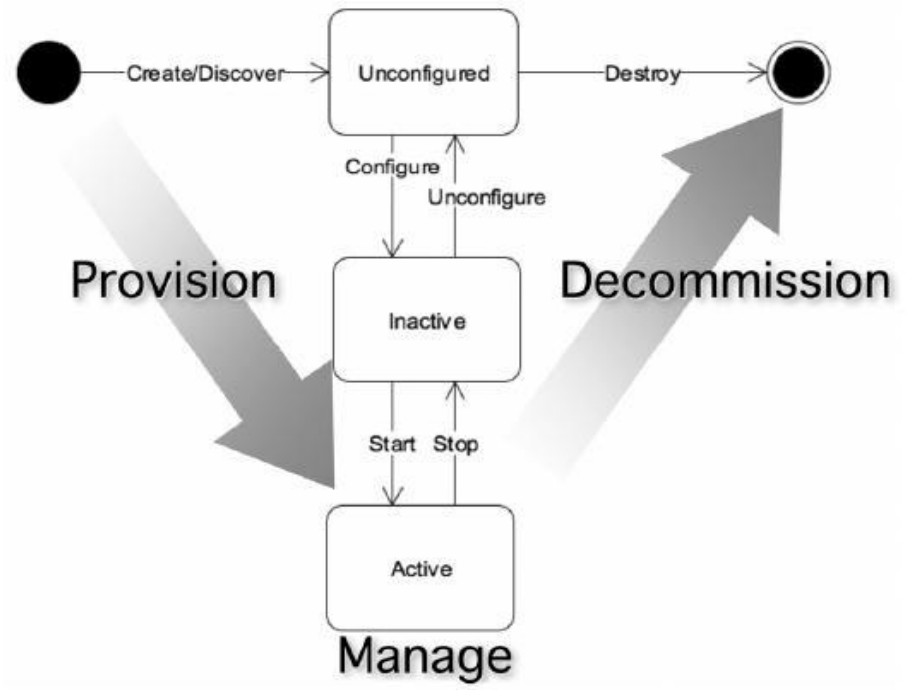

Figura 5 – Ciclo de vida geral de um componente de grid

Abastecimento - Abastecer um Grid envolve ações de criação e adição de componentes, configuração do mesmo, e colocá-lo em estado ativo. A adição pode ser feita manualmente ou através de aplicações que façam uma varredura programada para descobrir componentes a serem adicionados aos grid. Enquanto o processo de agregação e varredura deve incluir uma forma de autenticação mútua que garanta a relação de confiança entre as

partes envolvidas, a parte de configuração do componente deve incluir uma série de questões relativas à segurança do mesmo. Já colocá-lo em estado ativo pode considerar várias situações como, por exemplo, até mesmo fazer com que usuários, administradores e alguns serviços não sejam autorizados a colocar ou retirar um componente de seu estado ativo. Entre os pontos relativos à segurança que devem ser observados, podemos citar:

- QUEM (usuário ou aplicação) pode abastecer, abasteceu ou tentou abastecer um dado componente de Grid ?
- QUANDO o componente de Grid foi abastecido (para propósito de contabilidade) ?
- QUAL é o histórico de abastecimento de um componente de Grid (para propósito de auditoria) ?
- QUAL era o estado do componente de Grid antes de ser abastecido ?
- O componente de Grid foi verificado após o abastecimento para que se assegurasse sua integridade, níveis de segurança e estado desejado ?
- O software utilizado no abastecimento do Grid era confiável, vinha de fonte segura, continha algum código malicioso ?
- Todas as dependências necessárias foram atendidas antes do abastecimento ?

Administração contínua - A administração contínua de um componente de Grid envolve qualquer atividade de gerenciamento enquanto o componente está em estado ativo. Quando um componente não está abastecido (consequentemente, não ativo), nenhuma ação de gerenciamento (exceto o próprio abastecimento) pode ser realizada no componente, ou seja, o monitoramento é um ciclo que depende de um abastecimento bem sucedido do componente de Grid onde uma relação de confiança foi estabelecida entre o GME, o componente de Grid e suas partes envolvidas. Os comandos de gerenciamento devem ser seguros o suficiente, onde o componente de Grid confia em sua origem. Entre os pontos de segurança a serem observados no componente, podemos destacar:

- QUEM tem autoridade de criar, remover ou modificar tarefas administrativas e componentes de Grid ?
- A partir de onde os administradores podem realizar funções de gerenciamento ?
- Quais tarefas administrativas foram craiadas, modificadas ou removidas ? Quando ? Por quem ?
- QUEM (usuário ou aplicação) pode gerenciar os componentes de Grid e seus atributos de segurança ?
- QUEM pode definir as relações entre os componentes de Grid ?
- Que atributos de segurança podem ser gerenciados em um componente de Grid ? Quais foram modificados ? Quando e por quem ?
- De que maneira os atributos de segurança e as políticas estabelecidas podem ser distribuídos ou atualizados de forma segura em componentes de Grid participantes de ambientes heterogêneos ?
- Pode a entidade de gerenciamento do Grid usar tanto atributos comuns como outros específicos (relacionados a fabricantes) na definição de requisitos ou tomada de decisões ?
- Como a configuração de segurança de um dado componente de Grid é validada ? Há um padrão de checagem ?
- Quais são as repercussões no caso de falhas ? Há algum tipo de processo (manual ou automático) na detecção e recuperação de falhas ? Como os administradores serão notificados de uma falha de segurança ?
- Como os usuários se autenticarão nos componentes de Grid ? Que mecanismos utilizarão para acessá-los ?
- Que tipo de comunicação de rede será permitida para a entrada e saída de um componente de Grid ? Quem decide este tipo de comunicação ?
- Como conter as brechas de segurança de um componente de Grid ?

Desativação / reaproveitamento - A desativação de um componente de Grid pode ser dividida em três fases: parar, desconfigurar e remover um componente de grid. A desativação de um serviço ou a própria remoção de um componente de Grid que está obsoleto pode ser uma das razões para iniciar-se um processo de desativação de um componente de grid. Esta desativação também poderá ocorrer para que um componente de Grid seja reaproveitado, já que poderá ser abastecido novamente com outras características. Entre os pontos de segurança a serem observados nestas ações, destacam-se:

- QUEM (usuário ou aplicação) pode desativar / reaproveitar os atributos de segurança de um dado componente de Grid ? QUEM tentou realizar estas operações ?
- Que recursos foram desativados / reaproveitados ? Quando ? Por quem ? (para fins de contabilidade e auditoria)
- Há algum tipo de log, material criptografado ou dado para forensic capturado anteriormente ao desativação / reaproveitamento do recurso ?
- Sob que condições um recurso pode ser desativado / reaproveitado ? Há requisitos ou limitações relacionados a localização, serviços e / ou usuários ?
- Todas as dependências foram satisfeitas anteriormente ao desativação / reaproveitamento ?

4.3.1.3 Segurança da entidade de gerenciamento do grid

O modelo de referência da EGA define a Entidade de Gerenciamento de Grid (*Grid Management Entity - GME*) como a entidade lógica que gerencia os componentes de grid, as relações entre eles e todo o seus ciclos de vida (do abastecimento até o desativação). Na realidade, a GME pode ser uma combinação de pessoas, processos e tecnologia envolvidas. Apesar de ser algo logicamente separado da realização do Grid em si, a GME faz parte do todo, uma vez que, entre suas tarefas, ela é responsável pela definição, implementação e validação das políticas de segurança do grid. Aqui estão algumas responsabilidades da GME:

- Gerenciamento das identidades dos usuários;
- Autenticação das identidades;
- Gerenciamento do compartilhamento de serviços do grid;
- Captura, armazenamento (log), análise e informação de todo evento relacionado à segurança e auditoria;
- Gerenciamento (incluindo instalação , validação, armazenamento, destruição, etc...) de todas as chaves criptográficas usadas pelos elementos da arquitetura corporativa de grid;
- Implementação de comunicação segura através do ambiente de grid, incluindo acesso administrativo;
- Implementação de isolamento seguro de componentes de Grid compartilhados;
- Garantir que o gerenciamento local e remoto e operações de recuperação de falhas em toda a arquitetura de Grid se faz de forma segura e de acordo com as políticas de segurança adotadas pela organização;
- Validação individual ou de grupos de componentes de Grid que determine se eles estão em conformidade em relação à integridade, atributos, dependências, etc...

Enquanto os requisitos específicos de Grid corporativos associados com componentes individuais tem sido estudados, deve ser observado que a maioria daqueles requisitos focam na GME, *Grid Management Entity*. Isto é, em parte, resultado do papel exercido pela GME com respeito à definição de políticas , reforço e validação. Os recursos de Grid individualmente não são únicos em um ambiente de grid. O que é único é a maneira na qual eles estão agregados e gerenciados. Ao introduzir-se a figura do GME com capacidade de abastecer, gerenciar e desativar "pools" de recursos de grid, é possível chegar ao núcleo dos tipos de ameaças e requisitos de segurança de um ambiente de grid. Compreendendo e

mapeando estes tópicos, podemos tirar vantagens dos benefícios da centralização lógica do gerenciamento de segurança através da GME.

4.3.1.4 Ameaças e riscos em um ambiente de grid

O conceito de Segurança da Informação é relativamente novo e tem sido, aos poucos, incorporado pelos ambientes de trabalho. A figura do Security Officer e suas responsabilidades tem sido foco de discussão e adequação, principalmente, no ambiente corporativo.

Com a computação em grade não é diferente. Há uma necessidade real de análise e gerência dos riscos inerentes ao ambiente de Grid em questão. Para isto, devemos ter um entendimento das ameaças que estão envolvidas, sejam elas específicas ao ambiente corporativo ou não.

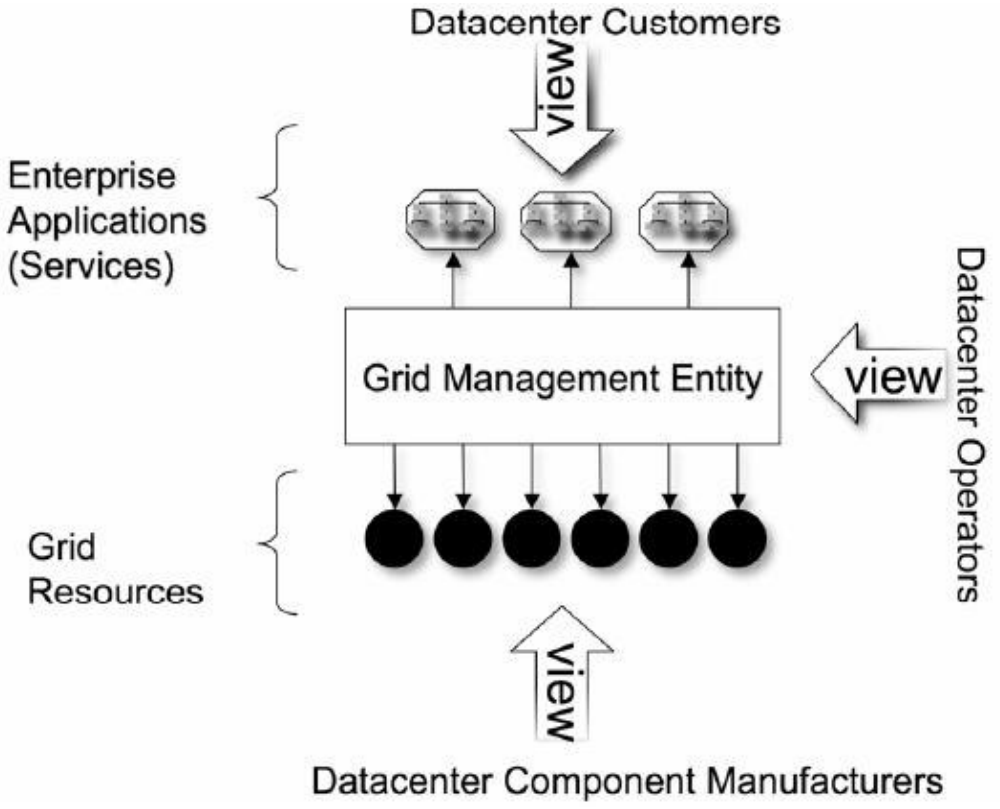

Figura 6 – Visão Básica de um Datacenter

No caso de Grid corporativos, e sob a ótica do que foi detalhado acerca das recomendações da EGA, a questão de segurança em um ambiente de Grid está relacionada diretamente em como o GME se comunica com recursos de Grid individuais ou de grupos para fazê-los trabalhar como se fossem um só (Figura 6). A GME é a entidade com poder e capacidade para saber sobre todos os recursos de Grid disponíveis e dizer a cada um deles o que fazer e quando fazer. Isto permite a cada participante ter sua chance de executar jobs no ambiente de grid. Além disso, o GME reforça , audita e valida a conformidade dos componentes de Grid a partir de pontos de políticas de segurança pré-definidas. O ciclo de vida de um componente de Grid deve ser também considerado quando tratamos da questão de ameaças e riscos.

Uma boa amostra de quais são os tipos de riscos e ameaças às quais os ambientes de Grid estão expostos segue abaixo:

Ataques ao controle de acesso, onde um usuário ou componente de Grid não-autorizado se une ao ambiente de grid; usuário ou serviço não-autorizado submete ou tenta submeter, monitorar ou controlar aplicações do grid; usuários ou serviços autorizados que invadem ou tentam invadir controles de acessos para aplicações e serviços disponíveis ou ainda tentam obter privilégios maiores do que os seus;

Ataques ao sistema de auditoria, para a violação da integridade de sistemas de auditoria e contabilidade relativos ao ambiente de grid. Inclui injeção falsa ou modificação de eventos, *overflow*, etc...;

Ataques de negação de serviço para indisponibilizar um serviço ou recurso. Enquanto grids corporativos geralmente oferecem melhor disponibilidade comparado

à outros ambientes , algumas ameaças de DoS devem ser consideradas para avaliação:

- Ataque de DoS contra a GME;
- Ataque de DoS contra o protocolo de adição do componente de grid, o qual permite que usuários ou componentes de Grid autorizados de unam ao ambiente de grid;
- Ataque que "force" que algum componente ou usuário abandone o grid;
- Ataques de DoS que inundam recursos e aumentam absurdamente o tráfego para gerar indisponibilidade, alta latência ou prejudicar o QoS do grid;
- Ataque que bloqueie ou modifique as mensagens da GME para os componentes de grid.

Códigos maliciosos ou *Malwares* que violam autorização de acesso e se auto-propaguem;

Ataque do tipo *Masquerade*, onde um falso componente de Grid se faz passar por um outro, válido no ambiente;

Ataque do tipo *Sniffer*, onde os dados trocados entre os componentes/usuários de Grid possam ser interceptados, violados e/ou modificados.

Além destas formas de riscos e ameaças, há outras categorias a serem consideradas que não são únicas do contexto de computação em grade, porém merecem comentário:

- **Segurança Física** – Um sistema de grid, como qualquer sistema de informação, necessita de proteção contra ameaças humanas (maliciosas ou acidentais) ou

desastres (naturais ou não). O uso de salas com acesso restrito e proteção contra incêndios ou ameaças da natureza pode ser uma medida interessante em casos de maior necessidade;

- **Engenharia Social** – A computação em grade não introduz um novo tipo de Engenharia Social ao modelo de ameaça existente em vários sistemas de informação. Como em toda política de segurança, medidas contra a eficácia desta prática devem ser tomadas e seguidas pelos usuários e administradores de um sistema de Grid;

- **Conformidade Regulatória** – É importante que as funções desempenhadas pelo sistema de Grid e seus usuários não violem qualquer lei governamental ou quebrem acordos industriais. Os requisitos de segurança que fazem parte das conformidades regulatórias devem ser incorporados à política do Grid, seus procedimentos e processos.

4.3.2 **Requisitos de segurança em ambientes de Grid**

Como já falado anteriormente, os requisitos de segurança em um ambiente de Grid devem ser baseados na política de segurança da organização. E, como já tem sido disseminado em cada vez mais empresas em todo o mundo, a política de segurança deve ser derivada de um exercício de avaliação de risco. Como em toda a avaliação de risco, a decisão final é o que fazer com este risco: diminui-lo, transferi-lo ou simplesmente aceitá-lo, baseando-se numa análise de impacto, custo e benefício. Os tópicos a seguir são requisitos comumente usados para reduzir os riscos e ameaças em um ambiente de Grid.

Confidencialidade, integridade, disponibilidade - Estes três requisitos básicos de segurança em qualquer sistema de informação se aplicam totalmente em um ambiente de grid. Na maioria das vezes, eles estarão presentes em cada funcionalidade de um componente de grid. Por exemplo, quando se falar em comunicação segura entre a Entidade gerenciadora do Grid (GME) e seus componentes (criptografia, não-repúdio, etc...), estará se falando de confidencialidade. E tal confidencialidade deve ser preservada através de todo o ciclo de vida dos componentes de grid, conforme já abordado anteriormente.

No momento em que se trata do processo de configuração dos componentes de grid, os valores a serem atribuídos dever ser validados por integridade. As mudanças destes controles devem ser poder da GME, e qualquer violação deve ser detectada por ela. E toda confidencialidade e integridade em um ambiente de Grid deve ser respaldada pelas política de segurança definida.

Disponibilidade não é apenas um requisito, mas uma necessidade de um sistema de grid. Por isso a necessidade de sua preservação , principalmente contra ataques do tipo DoS.

Identificação - Um pilar básico de sistemas de segurança é a habilidade de identificar tudo de uma forma única. Em um Grid corporativo, isto é aplicável em seus componentes e comunidades de usuários. Em particular, os componentes de Grid devem preservar suas identidades únicas através de todo o seu ciclo de vida, até mesmo em repetidas vezes em que for desativado ou reaproveitado. E mesmo se uma nova identidade é criada a cada vez que estes processos se repetirem, as identidades antigas devem ser gravadas para fins de auditoria e forensics. O GME , da mesma forma, deve ser identificado unicamente para que componentes de Grid e aplicações/serviços saibam com quem estão se comunicando.

Autenticação, autorização e auditoria - O chamado "triplo A" também se aplica ao ambiente de grid, garantindo maior segurança ao ambiente de grid. Cada entidade de comunicação deve poder se autenticar com a outra de forma segura, ser autorizado a se comunicar com a outra e ter ainda a possibilidade de auditar dados.

Separação de deveres, privilégio mínimo - Estes dois padrões de política de controle de acesso também se aplicam em um ambiente de grid, mais especificamente ao GME e aos administradores associados. Em alguns casos, isto pode fazer sentido para definir novos papéis ao administrador para suportar esta separação de deveres. Mesmo com novos papéis, todo e cada novo papel atribuído deve ser definido usando o conceito de privilégio mínimo (o chamado "need-to-know" e "need-to-have") como parte das boas práticas de segurança.

4.4 A FUSÃO ENTRE A EGA E O GGF

Em junho de 2006, a Enterprise Grid Alliance (EGA) e o Global Grid Forum (GGF) anunciaram sua fusão, formando, assim, o Open Grid Forum (OGF). A nova organização reune as duas organizações líderes nos padrões de Grid visando uma maior adoção de Grids. O OGF se beneficiará tanto do *expertise* e das práticas objetivas do EGA como da colaboração aberta para pesquisa, melhores práticas e desenvolvimento de padrões em Soluções de Grid do GGF. Ao unir os mundos da pesquisa científica ao mundo dos negócios, abrem-se portas para uma adoção comercial cada vez maior de soluções em Grid em todo o mundo. É, segundo seus próprios gestores, a reunião de interesses corporativos, dos governos e da comunidade acadêmico-científica, que juntam-se agora em um ambiente colaborativo, onde interoperabilidade é uma palavra cada vez mais forte.

4.5 CONECTIVIDADE E FIREWALLS

Enquanto a construção de um Grid requer, logicamente, uma conexão de rede entre todos os nós envolvidos, as políticas de segurança destas organizações virtuais, individualmente, podem bloquear parte ou a totalidade do tráfego necessário ao ambiente de Grid. Quando os recursos de um site pertencente à um ambiente de Grid está atrás de um Firewall, as políticas locais influem diretamente no uso do Grid, uma vez que estas regras, em geral, são configuradas sem a idéia de compartilhamento de recursos para a rede externa, no caso, a WAN. Considerando também o fato de que o Firewall torna-se um gargalo para aplicações distribuídas de Grid, já que alguns deles não estão preparados para tráfego de alta velocidade, novos problemas vêm à tona. Alguns questionamentos devem ser feitos:

- como uma organização virtual poderá permitir que os membros de uma ambiente de Grid acessem seus recursos sem comprometerem a segurança dos recursos restritos ao ambiente interno ?
- Uma vez que muitas instituições usam NAT e endereçamento IP privado (não válido), há um problema imediato com o nome do *host* a ser usado na troca de certificado. Qual devemos usar: o do *Firewall* ou o do *host* que compartilha o recurso ?

Para reduzir o risco ao expor suas máquinas internas, os administradores de cada organização virtual poderiam restringir o acesso à estas portas, filtrando por endereço IP de origem, por exemplo (no caso, endereços das outras organizações virtuais participantes do Grid). Entretanto, esta solução traz alguns problemas. Ela não funciona com pacotes UDP, porque ele contém um campo de endereço de origem que não é confiável, podendo ser facilmente manipulado por uma manobra de ataque do tipo *spoofing*, que burlaria o endereço IP de origem.

Devido ao aspecto dinâmico de um Grid, o administrador do *Firewall* teria que estar constantemente reconfigurando seu *Firewall* (de forma manual) a cada vez que um novo participante se associasse (ou deixasse) ao Grid. Além disto comprometer conceitualmente todo o esforço que as aplicações buscam no sentido de promover a facilidade de associação aos participantes de um Grid (pelo uso dos certificados digitais), ainda existe a possibilidade de ocorrer um erro eventual do administrador na reconfiguração do *Firewall*.

Algumas implementações poderiam trazer benefícios entre organizações virtuais participantes de um Grid em situações onde existissem Firewalls. Por exemplo, o uso do IPSEC *host* a *host*. Neste modo, o datagrama TCP estaria criptografado e o endereço de destino é deixado em texto claro. Isto pode ser útil quando a confidencialidade não é tão importante e o que se deseja saber é com quem estamos nos comunicando e se o dado não foi alterado. O modo de "tunelamento" é outra boa opção, estabelecendo uma comunicação segura entre dois Firewalls de organizações virtuais participantes. Neste caso, o datagrama TCP é criptografado bem como o endereço de destino. Um novo cabeçalho é usado, então uma VPN pode ser estabelecida entre dois *sites* remotos. O IPSEC fornece originalmente confidencialidade dos dados e autenticação usando:

- IP authentication header protocol (AH) ;
- IP Encapsulating Security Payload protocol (ESP) .

Ambos os protocolos requerem chaves secretas. Estas chaves são negociadas entre as partes comunicantes (VOs) usando o protocolo Internet Key Exchange (IKE). No ambiente de Grid, a autenticação originalmente fornecida pelo AH irá permitir que:

- Firewalls em organizações virtuais apenas aceitem pacotes originados de um endereço IP confiável e que pertence à um parceiro do Grid, uma vez que não é trivial o uso de *spoofing* no IPSEC;

- Seja fornecida proteção contra ataques do tipo *Denial of Service*, uma vez que o IP de origem é conhecido e confiável;
- Opere seguramente tanto em TCP quanto UDP.

O IPSEC também fornece confidencialidade pelo uso do protocolo ESP. Tanto o protocolo AH quanto o protocolo ESP podem ser usados sozinhos ou em conjunto para prover autenticação, confidencialidade ou ambos.

Na realidade, o uso de Firewalls entre organizações virtuais é, conceitualmente, contraditória à idéia do Grid de compartilhamento de recursos. Porém esta é uma realidade das redes atuais e os Forums de computação em grade consideram esta questão, tentando trazer soluções neste sentido. As ferramentas disponíveis prevêem a abertura de algumas portas ou *range* de portas e a aplicação deve ser informada exatamente acerca das portas abertas disponíveis e devem adaptar-se à este tipo de comunicação unicamente através delas.

A Tabela 1 mostra as portas que a versão 4 do Globus Toolkit solicita que sejam disponibilizadas em Firewalls:

Tabela 1 – Características de tráfego de rede do GT4

Application	Network Ports	Comments
GT4 GRAM (job startup and control)	To 8443/tcp on server from ephemeral port on client.	Connections back to client (controllable ephemeral port to controllable ephemeral port) required if executable or data staged from client or output from job sent back to client. Port 8443/tcp is default and configurable.
GT4 MDS	From ephemeral port on client to port 8443/tcp on service.	Same port as for GT4 GRAM.
GridFTP	From controllable ephemeral port on client to port 2811/tcp on server for control channel.	Port 2811/tcpdefined by IANA For information on data channel please see Section 3.3 Same as pre-WS GT.
GSI-Enabled SSH	From ephemeral port on client to port 22/tcp on server.	Same as standard SSH. Port 22/tcp defined by IANA.
MyProxy	From ephemeral port on client to port 7512/tcp on server.	Default. Can be modified by site.

Um agravante é o fato de alguns dos nós participantes de um ambiente de Grid estarem, além das regras de Firewall, utilizando o NAT, *Network Address Translator*. Se o NAT não suporta conectividade IP externa, isto também previne alguns tipos de aplicações. Em alguns casos poderíamos resolver este problema usando um gateway específico que fizesse o encaminhamento (*forward*) de informações considerando origem e destino dos nós participantes, mas isto significaria, sem contar a complexidade, uma grande degradação de performance, não se apresentando como uma real solução para o problema.

O elemento complicador do NAT reside na autenticação mútua entre um usuário e o recurso. Uma vez que que o recurso interno compartilhado aparece para a rede externa como

sendo o Firewall, temos um problema. O certificado de um recurso compartilhado em um Grid carrega um nome de *host*, o *hostname*. Da mesma forma que em sistemas de comércio eletrônico, no caso de recursos disponíveis atrás de *Firewalls* usando NAT, o usuário da organização virtual estará se conectando ao endereço público do *Firewall*, em uma porta específica. Além disso, o *hostname* do *Firewall* é esperado no certificado (FIGURA 7). O Firewall irá redirecionar a requisição ao recurso destino. Entretanto, os usuários não estarão aptos a se autenticarem no recurso porque o certificado não carrega o nome do recurso, ou seja, o nome real.

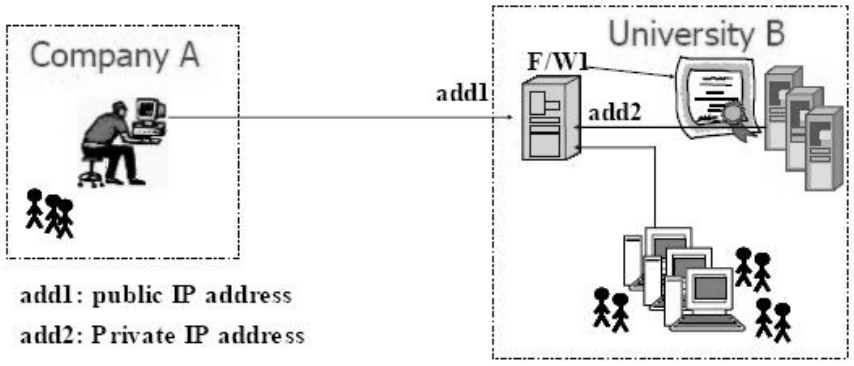

Figura 7 – O problema do NAT

A implementação de Firewalls entre organizações virtuais de um Grid é um problema, mas contornável em várias situações. O uso de perímetros diferenciados e específicos para cada finalidade (por exemplo, o perímetro para ambientes de Grid) é uma solução interessante, viabilizando tanto usuários remotos quanto usuários internos. Já o uso de endereçamento privado é uma questão sem solução adequada para integração de participantes em ambientes de Grid.

4.6 REDES IPV6 E OS AMBIENTES DE COMPUTAÇÃO EM GRADE

Sistemas de Grid são normalmente considerados como *middleware* de rede, uma vez que interagem aplicações e recursos de rede. Os dados em sistemas de Grid são transportados atualmente usando o IPV4. Mas a próxima geração do protocolo internet, o IPV6, já é uma realidade nas pesquisas sobre sistemas de Grid.

O período de transição entre o IPV4 e o IPV¨não será curto. Os sistemas de Grid devem operar em ambos os cenários e estarem aptos a se comunicarem em redes heterogêneas que falem ambos os protocolos. O diferenciador primordial de computação em grade de outros tipos de computação é o *middleware* usado. Ele é formatado de maneira a permitir que as aplicações rodem em clusters de computadores e em computação distribuída. O Global Grid Forum (GGF), tem também seu grupo de trabalho sobre o IPV6, desde a versão 3 do Toolkit. Chamado de “Global Grid Forum's IPv6 Working Group (GGF-IPv6-WG)”, este grupo estuda o impacto que o advento do IPV6 trará sobre a computação em grade, bem como o desenvolvimento e implementação de padrões e protocolos. Discussões acerca do uso do endereçamento, resolução de nomes e mapeamento de endereços IPV4 fazem parte do dia a dia deste grupo. E também há uma grande diferença em como em como o IPV4 e o IPV6 tratam a questão do NAT.

Enquanto escalabilidade, performance e heterogeneidade são objetivos desejáveis em qualquer sistema distribuído, incluindo Grids computacionais, as características dos ambientes de Grid os levam a busca pela segurança. Embora os avanços em termos de segurança que são inerentes do próprio protocolo IPV6 não resolvam os problemas neste aspecto, os Grids computacionais podem se beneficiar muito destas características. A segurança do IPV6 e das infra-estruturas de Grid ocorrem em níveis diferentes e podem ser empregadas juntas para prover um maior controle.

Os módulos de segurança em Grid referem-se, em alguns casos, ao endereço IP. Isto não causa nenhum problema em particular em um ambiente IPV4 ou IPV6 isolado. Eles podem, entretanto, causar problemas em ambientes híbridos. Enquanto é importante tirar vantagem das características do IPV6, todos nós temos consciência de que as redes IPV4 ainda irão existir por um bom tempo. Esta é a razão para considerarmos os ambientes híbridos IPV4 e IPV6 como uma questão a ser tratada.

Um esforço para integrar IPV6 em sistemas de Grid passa por uma abordagem independente do protocolo IP, que suporte ambas as versões. Segundo estudiosos da Universidade do Departamento de Ciência da Computação da University College London (Sheng Jiang, Piers O'Hanlon and Peter Kirstein), um servidor independente tem que ser apto a responder às chamadas de acordo com a versão do protocolo usada pelo cliente. Em outras palavras, o cliente decide qual versão de IP deve ser usada e este servidor do Grid responde ao cliente de acordo com a versão do protocolo IP que ele escolheu. Isto pode ser feito através de interfaces IPV4 e IPV6 neste servidor, chamado de "*Dual-Stack Server*". Os serviços HTTP, FTP, DNS, SSL, roteamento, entre outros, por exemplo, devem ser disponibilizados através de um *Dual-Stack Server*, garantindo o bom funcionamento de um ambiente de Grid.

Nâo é objeto deste estudo detalhar como é feita a tradução dos cabeçalhos entre o IPV6 e o IPV4 no sentido de, por exemplo, preservar o campo de *payload* do pacote. O importante é deixar claro que há buscas reais de soluções no sentido de proporcionar interoperabilidade entre ambientes heterogêneos.

5 CONCLUSÕES

A pesquisa proporcionou a percepção de que a adoção da computação em grade é uma preocupação real das organizações. No mundo cada vez mais globalizado e necessitando de recursos compartilhados de forma rápida, de alocação dinâmica e confiável, a computação em grade entra como uma tecnologia fundamental para integração de múltiplos domínios administrativos. E questões como tolerância à falhas, disponinibilidade, confiabilidade e integridade, palavras de ordem na área de segurança de qualquer organização, entram como requisitos básicos nesta adoção.

Para isto, foi possível ver o grande interesse comum que une o mercado corporativo, a área acadêmico-científica e governos em geral em comitês e forums acerca deste assunto: garantir compartilhamento confiável de recursos. Tanto isto é verdade que comitês de interesses nativamente científicos (como o GGF) e outros de interesses nativamente corporativos (como a EGA) resolveram unir esforços e interesses (com a criação do OGF) na solução de questões comuns, entre elas a segurança.

Este estudo sobre aspectos de segurança em computação em grade, ao mesmo tempo em que levanta questões, indica tendências e comprova a transformação dos ambientes de Grids computacionais, corrobora o uso de algumas técnicas já amplamente utilizadas nestes ambientes. A autenticação através de certificados X.509 é interessante e continua sendo uma aposta para a garantia de uma autenticação confiável de usuários em ambientes de Grid. Mas isto requer, de fato, a existência de uma infra-estrutura de chave pública (PKI) extremamente eficiente, onde, no mínimo, haja uma confiança mútua no nível de autoridades certificadoras. A conexão de dois Grids sem uma consulta prévia às CAs envolvidas pode tornar-se, efetivamente, um grande problema.

Entre as muitas técnicas interessantes que se apresentam, a identificação de cada nó participante de uma ambiente de Grid nos Firewalls das organizações e o consequente "tunelamento"com o protocolo IPSEC sugere uma boa solução, ainda que, de certa forma, engesse o compartilhamento de recursos entre as unidades previamente conhecidas. A questão da alocação dinâmica fica, num primeiro momento, comprometida, mas este é um ótimo começo para uma popularização dos Grids.

O conceito de "Ciclo de vida" para um Grid também se aprsenta como uma caminho bastante interessante no que tange a "validade" atribuída ä um componente de Grid, considerando as variáveis discutidas no capítulo dedicado às propostas da EGA. Amarrado com os requisitos tradicionais de segurança, esta é uma técnica que pode, também, alavancar a popularização de Grids no mercado corporativo, nicho ainda resistente à adoção dos Grids mas foco direto dos grandes fabricantes de software e hardware, que vêem neste mercado grandes oportunidades de negócio.

Outro grande problema atual é, sem dúvida, o fato de muitas organizações usarem endereços não válidos em segmentos de suas redes, ou por falta de endereços válidos disponíveis, ou como uma conclusão de que se trata de um elemento a mais de segurança para suas redes internas. Como a autenticação *host* a *host* fica "mascarada" nesta situação, e é extremamente complexo saber se o solicitante é realmente quem ele diz ser, a adoção do protocolo IPV6 se apresenta como a grande solução para esta questão, fazendo desaparecer o problema decorrente do uso do NAT. Com endereços IP válidos suficientes, e a desmistificação de que uma rede com endereçamento IP inválido significa uma rede "mais segura", esta será mais uma razão para a adoção e confiabilidade dos Grids computacionais.

Ainda sobre a adoção do IPV6, a migração do *middleware* de Grid para estas redes tende a ser satisfatória. O Globus Toolkit já prevê o uso do IPV6 desde sua versão 3 (é bom lembrar que o Globus já está na sua versão 4), e os mecanismos utilizados no Globus podem perfeitamente se adequar à outros sistemas de Grid. Há documentos *on-line* do tipo "*HowTo*" disponíveis oficialmente no endereço do Globus dentro de sua documentação de referência, o que irá facilitar muito aos admistradores nesta tarefa.

Uma frase de Foster de 2002, inserida no Referencial Teórico, profetiza, conceitualmente, o que está de fato ocorrendo no processo de uma maior adoção da tecnologia da computação em grade ao longo destes anos: "No futuro, para que instituições façam parte de grades precisarão implementar os protocolos OGSA, tal como para fazer parte da Internet hoje uma entidade precisa 'falar' IP". Mesmo que haja uma explícita citação ao OGSA, o que não está em discussão, o que esta afirmação prevê, e também é o que foi apontado como tendência nesta pesquisa, é que a padronização é o caminho para a interoperabilidade segura entre diferentes domínios administrativos. Da mesma forma que o IP garante a comunicação total entre diferentes arquiteturas de rede nos dias de hoje, algo inimaginável para a ARPANET nos anos 70, a comunicação segura de Grids computacionais segue para a padronização do *middleware.* Com isso e uma relação confiável entre diferentes domínios, a alocação dinâmica de recursos tende a ser uma realidade, facilitando a interoperabilidade de ambientes, com transparência para o usuário do Grid.

Mas construir um ambiente de Grid é uma tarefa muito complexa, que ainda requer uma grande intervenção manual por parte dos seus administradores. A complexidade ainda aumenta se considerarmos uma construção de baixo para cima, onde a conexão com recursos heterogêneos e administrados por unidades diferentes visando um ambiente distribuído. Quando estes recursos pertencem à ambientes de Grid, os problemas devem ser solucionados

uma a um. Mesmo o uso de um *middleware* único, como falado anteriormente (o Globus, por exemplo), não significa que dois Grids serão interoperáveis. Atualmente, o uso de versões iguais deste *middleware* não garante que as configurações serão compatíveis. Quando acrescentamos a questão de segurança, onde universos bastantes distintos de políticas e regras são aplicadas, é possível concluir que a interoperabilidade segura de dois ou mais ambientes de Grid passa por uma grande complexidade, que demanda profissionais qualificados e, acima de tudo, um grande bom senso na integração de interesses, onde o objetivo comum deve ser o compartilhamento de recursos computacionais.

"Bom senso" é o que os Forums e comitês que discutem a maior abrangência de uso dos Grids computacionais tentam buscar entre seus participantes. É exatamente o que também faz muitos *Frameworks* de boas práticas em Tecnologia da Informação se popularizarem no mercado atual, uma vez que a segurança é tratada atualmente como ponto estratégico pelas organizações em todo o mundo. Independentemente do fato dela ter fins lucrativos ou não, a questão da segurança entra como elemento primário no alinhamento da área de TI com o negócio, a atividade fim da organização. Sendo assim, é fundamental que o compartilhamento de recursos entre organizações virtuais passe por um processo de entendimento entre seus administradores e gestores visando a unificação de interesses, uma vez que isto é um ponto fundamental para a criação de políticas transparentes e, consequentemente, uma arquitetura mais consistente e segura para todos os usuários de Grids computacionais. Segundo o ITIL (Information Technology Infrastructure Library, da OGC – Office of Government Commerce), um *Framework* muito adotado na gestão de serviços de TI, um processo é definido como "uma série conectada de ações, atividades, mudanças, etc..., executadas por agentes com o intuito de satisfazer um propósito ou atingir um objetivo". Nos dias de hoje, diálogo e bom senso, unidos às técnicas de segurança, muitas delas discutidas aqui neste estudo, são fundamentais para este processo que vivemos da disseminação de uma tecnologia

que tem tudo para suprir, em curto prazo, nossas necessidades cada vez maiores por recursos computacionais globalizados e em tempo real.

6 **REFERENCIAL BIBLIOGRÁFICO**

ANDRADE, Nazareno. Reputação Autônoma como Incentivo à Colaboração no Compartilhamento de Recursos Computacionais. Dissertação de Mestrado. Campina Grande: Universidade Federal de Campina Grande, março 2004.

ANDRADE, Nazareno; CIRNE, Walfredo; BRASILEIRO, Francisco; ROISENBERG, Paulo. Ourgrid: An approach to easily assemble Grid with equitable resource sharing. In: 9th Workshop on Job Scheduling Strategies for Parallel Processing, Seatle, junho 2003.

ARAÚJO, Eliane; CIRNE, Walfredo; MENDES, Gustavo. Hiding Grid Resources Behind Brokers. Disponível em: <http://walfredo.dsc.ufcg.edu.br/papers/HidingGridResources.pdf>. Acesso em 15 mai. 2005.

BROWN, Martin. Develop your Grid service with the IBM Grid Toolbox. Disponível em <http://www-128.ibm.com/developerworks/grid/library/gr-develop/index.html>. Acesso em 15 mai. 2005.

CARVALHO, Osvaldo. GT Middleware . Disponível em <http://www.rnp.br/pd/gts2004-2005/middleware.html>. Acesso em 18 mai. 2005.

CIRNE, Walfredo. Grids Computacionais: Arquiteturas, Tecnologias e Aplicações. In: ERAD 2003: 3ª Escola Regional de Alto Desempenho, p.103-134, Santa Maria, janeiro 2003.

CIRNE, Walfredo; BRASILEIRO, Francisco; SAUVÉ, Jacques; ANDRADE, Nazareno; PARANHOS, Daniel; NETO, Eliseu; MEDEIROS, Raissa. Grid Computing for Bag of Tasks Applications. In: Third IFIP Conference on e-Commerce, e-Business and e-Government, São Paulo, setembro 2003.

COSTA, Lauro et al. MyGrid: A Complete Solution for running Bag-of-Tasks Applications. In: 22º Simpósio Brasileiro de Redes de Computadores (SBRC 2004), Gramado, maio 2004.

CRESWELL, John W. Research design: qualitative & quantitative approaches. Thousand Oaks: Sage, 1994

CZAJKOWSKI, Karl. et al. A Resource Management Architecture for Metacomputing Systems. In: IPPS/SPDP'98: Workshop on Job Scheduling Strategies for Parallel Processing. P. 62-82, Orlando, março 1998.

CZAJKOWSKI, Karl. et al. Grid Information Services for Distributed Resource Sharing. In: 10th IEEE International Symposium on High-Performance Distributed Computing (HPDC-10), IEEE Press, São Francisco, 2001.

The DataGrid Project. Disponível em: <http://www.edg.org> . Acesso em 22 jun. 2005.

The DataTag Project. Disponível em: <http://www.datatag.org> . Acesso em 22 jun. 2005.

FERREIRA, Luís et al. Globus Toolkit 3.0 Quickstart. IBM
RedPaper. Disponível em: <http://www-1.ibm.com/grid/grid_education.shtml> . Acesso em 22 jun. 2005.

FOSTER, Ian. What is the Grid? A Three Point Checklist. Grid Today, vol. 1, no. 6, julho 2002. Disponível em: <http://www.gridtoday.com/ 02/0722/100136.html> . Acesso em 24 jun. 2005.

FOSTER, I. et al. A Security Architecture for Computational Grids. In: 5th ACM Conference on Computer and Communications Security Conference, p. 83-92, São Francisco, 1998.

FOSTER, Ian; KESSELMAN, Carl; TUECKE, Steven. The anatomy of the Grid: Enabling Scalable Virtual Organizations. International J. Supercomputer Applications, 2001. Disponível em: <www.globus.org/research/ papers/anatomy.pdf> . Acesso em 27 jun. 2005.

FOSTER, Ian et al. The Physiology of the Grid: An Open Grid Architecture for Distributed Systems Integration. Disponível em: <http://www.globus.org/research/papers/ogsa.pdf> . Acesso em 14 jul. 2005.

FOSTER, I. et al. The Open Grid Services Architecture, Version 1.0. Disponível em: <http://forge.gridforum.org/projects/ogsa-wg> . Acesso em 18 mai. 2005.

Global Grid Forum. Disponível em <http://www.gridforum.org> . Acesso em 15 mai. 2005.

The Globus Alliance. Disponível em: <http://www.globus.org> . Acesso em 16 mai. 2005.

Grid Café. Disponível em: <http://gridcafe.web.cern.ch> . Acesso em 19 mai. 2005.

GRID.ORG – Grid Computing Projects. Disponível em: <http://www.grid.org>. Acesso em 21 mai. 2005.

HPTC Grid Computing. Disponível em: <http://www.hp.com/ techservers/grid/index.html>. Acesso em 22 ago. 2005.

IBM Grid Computing. Disponível em <http://www.ibm.com/grid>. Acesso em 22 ago. 2005.

The Internet Engineering Task Force. Disponível em <http://www.ietf.org> . Acesso em 23 ago. 2005.

KUSNETZKY, Dan; OLOFSON, Carl. Oracle 10g: Putting Grids to Work. Disponível em <http://www.oracle.com/technology/tech/grid/collateral/idc_oracle10g.pdf>. Acesso em 27 ago. 2005

Legion Worldwide Virtual Computer. Disponível em: <http://legion.virginia.edu> . Acesso em 16 jul. 2005.

LITZKOW, M.; LIVNY, M.; MUTKA, M. Condor – a hunter of idle workstations. In: 8th International Conference of Distributed Computing Systems, p. 104-11, 1988.

Manual MyGrid. Disponível em <http://www.ourgrid.org> . Acesso em 16 mai. 2005.

NAGARATATNAM, Nataraj et al. Security Architecture for Open Grid Services. Disponível em: <http://www.globus.org/ogsa/Security/draft-ggf-ogsa-sec-arch-01.pdf > . Acesso em 25 jul. 2005.

Oracle Database. Disponível em: <http://www.oracle.com/database> . Acesso em 19 mai. 2005.

OurGrid Project. Disponível em: <http://www.ourgrid.org> . Acesso em 15 mai. 2005.

RFC 3198: Terminology for Policy-Based Management. Disponível em: <http://www.ietf.org/rfc/rfc3198.txt?number=3198> . Acesso em 21 mai. 2005.

PEARLMAN, L. et al. A Comunity Authorization Service for Group Collaboration. In: IEEE 3rd International Workshop on Policies for Distributed Systems and Networks, 2002.

PEARLMAN, L. et. al. The Community Authorization Service: Status and Future. In: Conference for Computing in High Energy and Nuclear Physics (CHEP 03), La jolla, março 2003.

SELLTIZ, C. *et al.* Métodos de Pesquisa nas Relações Sociais. São Paulo: E.P.U., 1975, cap. 7

SOTOMAYOR, Borja. The Globus Tookit 3 Programmer's Tutorial. Disponível em: <http://www.casa-sotomayor.net/gt3-tutorial> . Acesso em 23 ago. 2005.

SUN Grid Computing. Disponível em: <http://wwws.sun.com/software/grid> . Acesso em 29 mai. 2005.

ORACLE 10g . Disponível em <http://www.oracle.com/grid>. Acesso em 10 jul. 2005

TANENBAUM 1996) Tanenbaum, Andrew. Computer Networks, 4th Edition. Prentice Hall. 2003.

TUECKE, S. et al. Open Grid Services Infrastructure (OGSI) Version 1.0. Disponível em: <http://www.ggf.org/documents/final.htm> . Acesso em 30 set. 2005.

VERGARA, Sylvia Constant. Projetos e relatórios de pesquisa em Administração, São Paulo: Atlas, 1997.

VERÍSSIMO, Paulo; RODRIGUES, Luís. Distributed Systems for System Architects. Massachusetts: Kluwer, 2000. p.401-402.

WELCH, Von et al. Security for Grid Services. In: Twelfth International Symposium on High Performance Distributed Computing (HPDC-12), IEEE Press, Junho 2003.

WELCH, Von et al. Use of SAML in the Comunity Authorization Service. Disponível em: <http://www.globus.org/Security/cas/Papers/ SAML Feedback-aug19.pdf> . Acesso em 31 nov. 2005.

WELCH, Von et al. X.509 Proxy Certificates for Dynamic Delegation. In: 3rd Annual PKI R&D Workshop, Gaithersburg , abril 2004.

ENTERPRISE GRID ALLIANCE. Enterprise Grid Security Requirements. Disponível em <http://www.gridalliance.org> . Acesso em 10 dez. 2005.

LANG, Bo et al. A Multipolicy Authorization Framework for Grid Security. Accepted by the IEEE NCA06 Workshop on Adaptive Grid Computing (to appear in Proc. Fifth IEEE Symposium on Network Computing and Application), Cambridge, USA, Junho 2006.

WELCH, Von et al. Security for Grid Services. Twelfth International Symposium on High Performance Distributed Computing (HPDC-12), IEEE Junho 2003.

CANON, Shane et al. Using CAS to manage role-based VO sub-groups.. In Proceedings of Computing in High Energy Physics 03 (CHEP '03), 2003.

FOSTER, Ian. The Community Authorization Service: Status and Future. In Proceedings of Computing in High Energy Physics 03 (CHEP '03), 2003.

Fine-Grain Authorization for Resource Management in the Grid Environment. K. Keahey, V. Welch. Proceedings of Grid2002 Workshop, 2002.

A Community Authorization Service for Group Collaboration. L. Pearlman, V. Welch, I. Foster, C. Kesselman, S. Tuecke. IEEE 3rd International Workshop on Policies for Distributed Systems and Networks, 2002.

An Online Credential Repository for the Grid: MyProxy. J. Novotny, S. Tuecke, V. Welch. Proceedings of the Tenth International Symposium on High Performance Distributed Computing (HPDC-10), IEEE Press, agosto 2001.

WELCH, Von et al. A National-Scale Authentication Infrastructure.. IEEE, 2000.

FOSTER, Ian et al. A Security Architecture for Computational Grids.. Proc. 5th ACM Conference on Computer and Communications Security Conference, pp. 83-92, 1998.

FOSTER, Ian et al. Managing Security in High-Performance Distributed Computing.. Cluster Computing, 1(1):95-107, 1998.

Jiang, Sheng et al. Moving Grid systems to IPV6 era. Disponível em <http://www.cs.ucl.ac.uk/staff/sjiang/publications/Moving_Grid_Systems_into_the_IPv6_Era.pdf> . Acesso em 15 abr. 2006.