

# Protegendo o seu Servidor Firebird

## Procedimentos para uma Instalação Segura

Autor: Mark O'Donohue Tradução/Adaptação: Paulo Vaz

### Introdução

*Segurança em banco de dados tem sido uma constante preocupação dos desenvolvedores e dos administradores de sistemas. O Firebird tem sido alvo de algumas críticas, pois apesar de privilegiar os recursos de processamento, deixa a desejar no aspecto de segurança.*

*No entanto, muito se pode fazer, através do conhecimento das técnicas que podem ser aplicadas para melhorar e até resolver estes problemas. Este artigo se propõe a dar esta visão.*

*Os itens em caracteres itálicos são adições e adaptações ao artigo original.*

### Visão Geral

O Firebird trabalha em três possíveis modos: acesso direto local, acesso pela versão Classic e mais recentemente acesso pela versão SuperServer.

Antes de examinarmos as questões de segurança é importante determinar qual o modo ou modos que você irá utilizar.

Daqui em diante sempre que nos referirmos aos "Arquivos de Sistema do Firebird" estaremos nos referindo aos arquivos de banco de dados de usuários `isc4.gdb`, `isc_event1.<nome do host>`, `isc_init1.<nome do host>` e `isc1_lock1.<nome do host>` todos pertencentes à plataforma Linux normalmente encontrados no diretório `/opt/interbase`.

Tenha em mente que este artigo é voltado primariamente para as plataformas Linux/Unix, embora o material possa ser útil em plataformas Windows.

### Acesso direto Local

O método mais eficiente de acesso ao Firebird é o acesso direto local, neste modo o motor de acesso ao banco de dados, roda com os privilégios do usuário corrente executando uma aplicação, que acessa direta e localmente todos os arquivos de sistema do Firebird e o banco de dados.

### Trabalhando com o Classic Server

É possível com a versão Classic trabalhar com usuários locais e remotos ao mesmo tempo. O gerenciamento de bloqueios e outros aspectos relacionados serão controlados automaticamente pelo motor do banco de dados.

*Utilizando-se a versão Classic em acesso local, é possível fazer acesso direto aos arquivos do sistema do Firebird, portanto todos os nomes de usuários do Unix utilizados nos processos do servidor (incluindo aqueles processos-filhos que recebem nomes distintos) precisam ter acesso aos arquivos de Sistema do Firebird.*

A versão Classic Server registra-se como um serviço Linux, e cada cliente que efetua uma conexão remota na máquina servidora utilizando a porta 3050, divide este serviço como processos-filhos.

Cada processo atende às requisições de um cliente remoto específico. Uma única máquina pode suportar muitos processos separados de clientes, que serão executados concorrentemente (multitarefa).

Em caso de acesso remoto, dependendo da número de usuários, pode-se criar um grupo de usuários, inserindo-os nele. O importante é ter em mente que estes usuários que rodam estes processos no servidor (inclusive seus processos-filhos) precisam acesso de leitura e gravação aos arquivos do Sistema do Firebird.

### Trabalhando com o SuperServer

Mais recentemente uma arquitetura multi-tarefa foi implementada, onde todas as tarefas separadas do servidor compartilham o mesmo espaço, sendo possível várias tarefas serem usadas em uma única requisição de cliente.

Neste modo o servidor roda como um usuário privilegiado (usualmente como root/firebird/interbase ou interbas) e somente este usuário precisa acesso aos arquivos de Sistema do Firebird.

*A versão SuperServer é a única disponível para a plataforma Windows. No Linux estão disponíveis a versão Classic e SuperServer.*

### **Sugestões para uma Configuração Segura**

As sugestões abaixo aplicam-se à ambas versões do Firebird (Classic e SuperServer). Vamos à lista:

1. Certifique-se que as definições de UDFs podem ser feitas apenas por usuários confiáveis.

Uma UDF roda no mesmo espaço e com os mesmo privilégios do Servidor. É importante que qualquer UDF disponível no Firebird possa ser instalada e estar disponível apenas por/para usuários e administradores confiáveis.

2. Certifique-se que tabelas externas só possam criadas/acessadas por usuários confiáveis.

É possível que no projeto do banco de dados, existam tabelas externas. Quando o firebird estiver rodando em um servidor que permita acesso à estas tabelas diretamente por usuários remotos, é importante certificar-se que estes usuários saibam que modificar estas tabelas pode comprometer a integridade do banco de dados.

3. Certifique-se que as máquinas clientes sejam confiáveis, e que cada usuário que acessa a máquina cliente é confiável.

Uma vez que o servidor Firebird confia na máquina cliente, há uma confiança explícita pelo servidor em todas as informações enviadas do/para o cliente.

Isto inclui às vezes informações privilegiadas como o nome do usuário na máquina cliente. Portanto é interessante identificar no servidor quais as máquinas que são confiáveis para o acesso ao servidor.

Também é possível que um usuário mal intencionado acesse uma máquina confiável, e alimente o servidor com informações incorretas e ganhe acesso privilegiado à bancos de dados no servidor. Isto deve ser evitado com restrição de acesso à estes equipamentos.

4. Se estiver rodando um servidor web ou aplicações multi-camadas tenha certeza de que sejam obrigatórios nome de usuário e senha para acessar o servidor.

Existem efeitos negativos de não serem utilizados nomes e senhas diferenciadas em ambientes web ou multi-camadas, podendo resultar em que alguém estranho consiga apropriar-se dos privilégios de acesso do cliente ou do processo do servidor.

A melhor maneira de evitar isto é certificar-se que um nome de usuário seja especificado explicitamente antes da chamada ao processo de cliente Firebird seja feita.

5. Use sempre o Firebird nunca o Interbase 6

*O Interbase 6 além de bugs contém uma 'back door' que permite acesso direto ao Banco de Dados. Mesmo havendo sido liberado um patch de correção, ainda sobram os demais bugs.*

6. Não rode o servidor como usuário root

O script de instalação do Firebird no Linux foi modificado para que não seja necessário a execução do Servidor como super-usuário (root).

*Verifique após a instalação, qual o usuário vinculado ao serviço e seus privilégios.*

*No Windows NT/W2K/XP a instalação precisa ser feita como Administrador do Sistema, não havendo a necessidade posterior do uso dele para o Firebird funcionar se utilizado como serviço.*

*Em máquinas Win9x/Me não restrições de segurança, não sendo portanto recomendadas para instalação de servidores seguros.*

#### 7. Modifique a senha do SYSDBA

A senha padrão do Sysdba 'masterkey' é muito conhecida e obviamente insegura. Para garantir a segurança, troque esta senha na primeira oportunidade.

O instalador do Linux poderá automaticamente fazer isto se desejado, e esta funcionalidade deverá ser implementada futuramente nas instalações para outras plataformas.

#### 8. As senhas são restritas à 8 caracteres, portanto são suscetíveis à "ataque de força bruta".

Tenha certeza de que o isc4.gdb só é visível aos usuários apropriados e utilize rotinas de monitoramento e travamento de tentativas de acesso incorretas repetidas.

O algoritmo de encriptação/desencriptação de senhas é baseado na velha tradição Unix usando apenas os 8 primeiros caracteres. Com o atual poder de computação, estas senhas são facilmente quebradas utilizando o "ataque de força bruta" (tentando todas as combinações até 8 caracteres).

Entretanto, um ataque deste tipo requer muitas tentativas de entrada de senha. Isto é feito mais facilmente "roubando-se" o arquivo de senhas (isc4.gdb) e tentando tudo remotamente ou ainda através de um servidor Web.

Restringindo a visibilidade do isc4.gdb, e colocando rotinas para monitorar e travar tentativas de acesso errado repetidas, poderão reduzir sua exposição à este problema.

#### 9. Troque as senhas regularmente e mantenha-as seguras.

A maior causa de quebra de segurança é facilitar o acesso às senhas. Tem gente que coloca o nome do usuário e senha em um adesivo colado no computador, ou escolhe a palavra "senha" como sua senha. Isto jamais deve ser feito para contas de usuários com mais poderes.

#### 10. Restrinja a comunicação entre clientes e o servidor em uma rede segura.

Muito da comunicação entre o cliente e o servidor contém informações importantes. E esta informação pode ser facilmente interceptada por alguém que "escute" as comunicações da sua rede.

Por exemplo, a senha criptografada é enviada do cliente ao servidor pode ser percebida por outro.

Então é importante certificar-se que o caminho na rede entre o cliente e o servidor é seguro, talvez pelo uso de tecnologias como o Firewall (parede-corta-fogo).

Existem produtos compatíveis com o Firebird disponíveis para prover um túnel encriptado entre o cliente e o servidor. *O mais conhecido é o Zebedee.*

#### 11. Mantenha o servidor atrás de um Firewall

Quando seu servidor está protegido, em uma rede segura, com as máquinas clientes confiáveis identificadas, não há mais coisas com as quais preocupar-se.

Entretanto, colocar suas máquinas servidoras atrás de um Firewall é sempre uma boa idéia. As razões disto são óbvias, e certamente você sabe por que.

#### 12. Mantenha os Clientes atrás de um Firewall.

Como mencionado anteriormente, o servidor confia nos processos do cliente, então é importante que a integridade do processo cliente não seja comprometida.

Novamente por razões óbvias, é interessante manter os processos dos clientes atrás de um Firewall.

### 13. Excesso de Buffers - Verifique os tamanhos dos campos utilizados em páginas Web.

Há um grande número de comandos de cópia de seqüências de caracteres no código do Firebird (strcpy, memcpy), que não verificam o tamanho dos dados que serão copiados.

Apesar de um grande número destes comandos serem seguros, e o uso destas funções não é recomendada pois são alvos de ataques aos Buffers do sistema.

É possível que algumas destas seqüências possam ser manipuladas externamente pela passagem de sequencias binárias de dados em declarações SQL ou forçar entradas aleatórias na porta 3050 do servidor.

É importante enfatizar aqui, que este é uma possibilidade de ataque desconhecida, mas que potencialmente ela pode existir.

E isto pode ser mais facilmente tentado se o servidor ou o cliente não estiver atrás de um Firewall, ou rodando em sistemas confiáveis.

O único modo de passar dados através do cliente para o servidor é via processos definidos no cliente, que podem estar em uma página Web em ASP ou JSP. Neste ponto, faça uma verificação adicional através de uma programação defensiva, verificando o tamanho dos campos entrados pelos usuários em uma página de entrada de dados Web (um nome de usuário > 8kb por padrão é provavalemente uma indicação que algo pode apresentar problemas)

### 14. Restrinja o acesso aos arquivos de sistema do Firebird à usuários conectados diretamente ao Servidor.

No modo de conexão remota, o usuário de trabalho não deve ter acesso físico direto para leitura e escrita ao banco de dados e aos arquivos de sistema do Firebird (compartilhamento de arquivos). Você deve restringir o proprietário e os direitos de acesso aos arquivos de sistema do Firebird à usuários que realmente possam acessá-los.

*Se necessário isole fisicamente o acesso ao servidor, colocando em uma sala separada, para evitar problemas de visitantes indesejados.*

Se você possui dois usuários de trabalho diferentes utilizando uma mesma conta em modo local, e se ambos trabalham com diferentes bancos de dados, ambos os usuários precisarão ter acesso de gravação aos arquivos de sistema do Firebird e às bases de dados.

Somente no modo de acesso direto, mesmo que o usuário tenha acesso completo de leitura e escrita, não será possível explorar nenhuma vulnerabilidade nos processos do servidor para obter privilégios adicionais, como não há processos remotos ativos no servidor para atacar.

### **Então o que pode ser considerado seguro?**

Por convenção - um servidor Web que conecta a um servidor Firebird, onde o servidor de banco de dados e o servidor Web são bem protegidos usando Firewalls e o servidor Web é chaveado, pode-se considerá-lo seguro, particularmente se o código (ASP ou JSP) utilizado verificar o tamanho das seqüências de dados passadas no software cliente do Firebird (talvez por verificar o tamanho da instrução SQL resultante). Assim o potencial de ataques é realmente mínimo.

Se você estiver rodando o Firebird atrás de um Firewall em uma rede local com um ou mais servidores, a muitas máquinas clientes então você precisa confiar que estes usuários de rede locais, são aqueles que rodam o software cliente esperado. Coisas simples como monitorar todo o tráfego de IP de acesso ao banco de dados, obtendo algumas informações relevantes sobre o usuário, e mostrando-se alguém enviando um ataque à porta 3050 tentando derrubar o servidor ou causar um estouro de buffer, podem dar conta.

Estes são os possíveis problemas que a maioria das aplicações em redes locais podem encontrar atualmente, então o Firebird não está sozinho aqui (isto não é uma desculpa, e isto certamente abre a necessidade de melhorias ).

## Soluções e Melhorias

Muito do que pode ser feito para melhorar os aspectos de segurança do Firebird, deverão ser tópicos para outras discussões.

Muitos dos pequenos aspectos, como melhorar o algoritmo de encriptação de senhas (em vez do padrão DEA, talvez seja adotado o SHA1 ou MD5), ou fazer a instalação no Linux não ser só a única que permite modificar em tempo de execução a senha do superusuário, são relativamente fáceis, necessárias e provavelmente inseridas em breve.

As questões maiores aqui relacionadas à autenticação de usuários e comunicação segura entre o cliente e o servidor, não são as únicas, e muitas outras boas soluções já existem em outros projetos open-source.

Minhas preferências são por utilizar a solução "Public Key Infrastructure" (PKI) para autenticação e SSL quando apropriado para comunicações seguras. Felizmente a maioria disto está disponível no projeto OPENSLL, e mais ainda, alguns de nós tem alguma familiaridade com isto através do seu predecessor, o projeto SSLEAY.

*A criação de ferramentas como o Zebedee vem complementar a funcionalidade do Firebird tornando-o seguro e rápido no uso em aplicações Web. Por não ser o escopo deste artigo, fica aí o registro de que vale a pena examinar a funcionalidade e as possibilidades de uso desta ferramenta.*

## Conclusão

A auditoria na segurança do Firebird continua, mas acreditamos que haverá futuramente soluções no projeto para resolver as limitações/problemas no sentido de tornar o Firebird um produto mais seguro e robusto disponível para o uso no mundo vulnerável da Internet atual.

Entretanto enquanto este trabalho não é concluído, podemos usar nosso tempo livre para ajudar a detectar estas vulnerabilidades, e nos precavermos assumindo que outros poderão também encontrá-las.

Por isto é importante que as pessoas que irão utilizar o Firebird tenham boas informações sobre como configurar e rodar suas instalações de forma segura.

Em adição aos pontos aqui sugeridos, e dando uma olhada na documentação disponível, pode ser muito útil participar em grupos de usuários e fóruns de discussão, que por enquanto, são a forma mais rápida de se saber as novidades, pois todas as informações significativas surgem nelas primeiro.

<p>Artigo Original:</p> <p><a href="http://www.ibphoenix.com/main.nfs?a=ibphoenixApp&amp;l=:IBPHOENIXAPP.PAGES:NAME='art_fb_security'">http://www.ibphoenix.com/main.nfs?a=ibphoenixApp&amp;l=:IBPHOENIXAPP.PAGES:NAME='art_fb_security'</a></p> <p><b>Mark O'Donohue</b></p> <p><a href="mailto:mark.odonohue@ludwig.edu.au">mark.odonohue@ludwig.edu.au</a></p>	
<p>Tradução e adaptação:</p> <p><b>Paulo Vaz</b></p> <p><a href="mailto:paulo@multi-informatica.com.br">paulo@multi-informatica.com.br</a></p>	<p><b>Comunidade Firebird de Língua Portuguesa</b></p> <p>Visite a Comunidade em:</p> <p><a href="http://www.comunidade-firebird.org">http://www.comunidade-firebird.org</a></p>

A Comunidade Firebird de Língua Portuguesa foi autorizada pelo Autor do Original para elaborar esta tradução.