



LPAULO@CHAMANDO.COM.BR
LUIZ PAULO DE OLIVEIRA SANTOS





10 anos de Firebird Fundação Ann Harisson Firebird 2.5 Firebird 3





Principais features:

Desativação de usuário invisível (direitos de ROOT) do IB6.

Padronização da porta 3050

CURRENT_USER e CURRENT_ROLE

Forced Writes ON como padrão no Win32

Nova ODS (On Disk Structure)





Principais features:

Em conformidade com o conceito A.C.I.D.

MGA: "Arquitetura de Múltiplas Gerações" (Multi-Generational Architecture)

Procedimentos Armazenados (Stored Procedures)

Eventos

Geradores (Generators)

Backups Online com GBak

Gatilhos (Triggers)

Integridade Referencial em Cascata (Declarative Cascading Referential Integrity)

Direitos de usuários e grupos para diretórios

SECURITY.FDB

GRANT e REVOKE

Aliases.conf

Firebird.conf

Shadows e replicação de base de dados





Principais features:

- Manutenção de usuários feita através de API
- Melhorias (sutis) no protocolo de comunicação
- Script para trocar a senha do usuário SYSDBA em:
 /opt/firebird/changeDBApassword.sh
- Implementação de cláusula WITH LOCK em comandos SELECT
- Melhorias no *Garbage Collector*
- Variável SYSTEM
- O comando: **gfix -shut -full**
- Back up incremental com NBACKUP
- 30% mais veloz em diversas situações
- SECURITY2.FDB
- Atualização do software do banco
- FB 2.0 com SHA-1.
- Nova ODS evita problema de disco cheio
- GSEC não mais exige [--server] nem path





No SECURITY.FDB:

SYSDBA,55gat5u

ZORRO,55gat5u

No SECURITY2.FDB:

SYSDBA,DSAS6787DF76DSD76

ZORRO,GGD767431AA097E886





Alex Peshkov

Rússia



Desenvolvedor que
organiza o time de
segurança do Firebird

What can I add here? Upgrade, please. FB 2.0 in average 30% faster compared with 1.5, supports popular AMD64 architecture, much secure, has a number of new interesting SQL features (insert returning values, for example) and a great list of fixed errors.

I know that firebird community in Brasil is very big, and may be some of you will take more active part in future versions development - software developers are always welcome, and we still suffer from missing good documentation.





Principais features:

Manutenção de usuários feita através de API
Autenticação melhorada principalmente no Windows
ExternalFileAccess - Para acesso à arquivos externos
Melhorias (sutis) no protocolo de comunicação

Script para trocar a senha do usuário SYSDBA em:

```
/opt/firebird/changeDBApassword.sh
```

Implementação de cláusula WITH LOCK em comandos SELECT

Melhorias no *Garbage Collector*

O comando: **gfix -shut -full**





Nova role RDB\$ADMIN na ODS 11.2 - permite o SYSDBA transferir seus privilégios para outro user.

Possibilidade de qualquer usuário "monitorar-se" com:
CURRENT_CONNECTION

Melhorias na API para shutdown.

Melhorias no NBackup





- **Físicos**
 - Invasão de recintos (instalações)
- **Lógicos**
 - Brute-force
 - Deny of Service
 - Spoofs / Sniffers / Pen
- **Psicológicos**
 - Engenharia Social
 - Coação / chantagens





- Invasão de prédios e instalações de servidores:
 - Com facilitação
 - Sem consentimento
- Principais problemas provocados pelo tipo:
 - Desaparecimento do hardware (base por consequência)
 - Danos Lógicos (formatação / outros congêneres)
 - Danos físicos (incêndio / danos intencionais / desastres)



Dica para evitar o problema:

Compre um sistema de alarme!





- Brute-force / Pentest
 - Descobrir Senhas
- Deny of Service / Pentest
 - Parar o serviço do Firebird
- Spoofs / Sniffers / Pentest
 - Capturar pacotes de informações que trafegam entre o servidor e a estação. Capturando informações importantes dos usuários. Dados cadastrados ou consultados

Dica para evitar o problema:

Firewall e IDS ativos e rede segmentada com switches e routers! Implementar bastion-hosts e LOGs!





- Engenharia Social:

- Através de artimanhas o intruso descobre informações e senhas dos usuários e administradores

- Coação / chantagens:

- Através de chantagem/benefícios algum usuário libera a senha para acesso ao banco de dados

Dica para evitar o problema:

Contratar funcionários confiáveis e impossibilitar o acesso fora do horário do expediente, tratar o lixo (rascunhos).





- Sniffers
 - Ferramentas para captura de pacotes de dados
- Zebedee (ZBD)
 - Criptografia e compressão
- VPN
 - Extensão de redes LAN em ambiente WAN
- Firewall
 - Instalado no servidor Firebird (IPTables)
- IDS
 - Sistemas de Detecção de Intrusão



Script para IPTables para bloquear Brute-Force



```
iptables -A INPUT -p tcp --syn --dport 3050 -m recent --name fbbforce --set
```

```
iptables -A INPUT -p tcp --dport 3050 --syn -m recent --name fbbforce --rcheck --seconds 60  
--hitcount 3 -j LOG --log-prefix 'FB DISCARD: '
```

```
iptables -A INPUT -p tcp --dport 3050 --syn -m recent --name fbbforce --rcheck --seconds 60  
--hitcount 3 -j REJECT --reject-with tcp-reset
```

```
iptables -A FORWARD -p tcp --syn --dport 3050 -m recent --name fbbforce --set
```

```
iptables -A FORWARD -p tcp --dport 3050 --syn -m recent --name fbbforce --rcheck --seconds  
60 --hitcount 3 -j LOG --log-prefix 'FB DISCARD: '
```

```
iptables -A FORWARD -p tcp --dport 3050 --syn -m recent --name fbbforce --rcheck --seconds  
60 --hitcount 3 -j REJECT --reject-with tcp-reset
```



Logando acessos ao FB (IPTables)



Para logar os acessos ao seu Firebird, instale o IPTables em seu servidor Firebird e execute a seguinte linha:

```
iptables -I INPUT 1 -m limit -p tcp --destination-port 3050 -j  
LOG --log-level 1 --log-prefix 'FB >'
```

Pode-se ler os logs armazenados no /var/log/syslog.

Exemplo de linha gerada após um acesso ao FB:

```
Jul 15 10:34:17 localhost kernel: FB >IN=eth0 OUT=  
MAC=00:1a:3d:66:20:f1:00:40:11:00:df:9f:28:10 SRC=10.1.0.11 DST=10.1.0.49  
LEN=342 TOS=0x00 PREC=0x00 TTL=128 ID=12194 DF PROTO=TCP SPT=3527  
DPT=80 WINDOW=17520 RES=0x00 ACK PSH URGP=0
```





Servidor Embutido ou Embarcado pode ser usado para acessar dados de banco Firebird (sem o uso de senhas).





OpenVAS ou Open Vulnerability Assessment System é uma ferramenta para teste de penetração (Pentest) em sua rede / servidor / serviços, e pode:

- * Indicar falhas – apontando melhorias
- * Provocar DOS – durante os testes
- * Certificar Brute-force

Aplique você mesmo em seu servidor ou procure um especialista no assunto!





Snort® é uma ferramenta Open Source para Network Intrusion Prevention e Intrusion Detection System (IDS/IPS).

Algumas de suas funções:

- Gerar Logs
- Permitir automatizar atitudes (com IPTables)
- Alertar os administradores de problemas
- Contabilizar uso da rede





- Sistema de arquivos criptografados:
 - TrueCrypt (OpenSource)
 - CYPHERIX Strong Encryption - Criptainer LE (Freeware)
 - PGP - Whole Disk Encryption (Comercial)
- Sistema de Arquivos Hidden
 - TrueCrypt (OpenSource)





As redes Wireless baseadas em redes abertas ou baseadas em privacidade baixa são extremamente frágeis e problemáticas.

Atualmente quebrar uma rede protegida por WEP com uma distro Linux (Backtrack ou DEFT) pode ser feito em menos de 15 minutos.

Dica para Wireless: ZEBEDEEE nelas!!!





Evite carregar qualquer ferramenta de administração de banco de dados com a IDE de desenvolvimento aberta, pois o sistema de depuração pode ser usado para capturar informações de outros aplicativos (endereçamento de memória).





O **SQL Injection** é o maior veneno enfrentado pelos desenvolvedores e analistas de segurança para bancos de dados. Deve ser tratado na aplicação (através de filtros) e no próprio banco.

Linguagens scripts são as mais susceptíveis à tal malícia. Portanto **CUIDADO!!!**



Os 10 mandamentos da segurança com FB



1. Não usarás jamais a senha **masterkey**, seja para o SYSDBA ou outro usuário.
2. Terás sempre back up atualizado, shadows e base replicada.
3. Usarás sempre o Zebedee, um firewall para proteger seu Firebird e um IPTraf para monitorar o acesso.
4. Não abusarás de U.D.F.s, e, principalmente de UDFs que você não criou!
5. Não utilizarás as variáveis ISC_USER e ISC_PASSWORD em vão.
6. Manterás o Hardware e sistema operacional atualizados.
7. Não atribuirás número IP válido e público ao servidor sem real necessidade.
8. Não deixarás faltar espaço no disco do seu banco de dados.
9. Contribuirás sempre com a Firebird foundation.
10. Comprará o livro “Firebird – Dicas de Segurança” e seguirá os passos à risca!



Dica para os participantes do FDD



Compre o livro **Firebird – Dicas de Segurança** no stand da Firebase por apenas R\$ 30,00.

Obrigado a todos e até a próxima...



Fim...



Perguntas???

