

IBSurgeon

FBDataGuard 2.8

Guia do Usuário

Versão 1.5.0

Table of Contents

FBDataGuard for Windows User Guide.....	4
1. What is IBSurgeon’s FBDataGuard?	4
About IBSurgeon	4
2. Installation.....	4
2.1. Download and registration.....	4
2.2. Installation on Windows.....	5
2.3. Choosing folders to store configuration, backups and statistics	6
2.4. Installation on Linux	7
3. Initial FBDataGuard Configuration	10
3.1. Launch web-console.....	10
3.2. Auto discovery feature of FBDataGuard	11
3.3. Firebird server registration	12
3.4. Firebird database registration.....	15
3.5. Email alerts in FBDataGuard.....	16
3.6. Next steps with FBDataGuard	18
3.7. Embedding FBDataGuard into your own application.....	18
4. Configuring FBDataGuard with Web-console	19
4.1. Overview of Web-console	19
4.2. Server: General configuration	20
4.3. Server: auto updates	21
4.4. Server: Agent Space	21
4.5. Server: Server version	22
4.6. Server: Server log	22
4.7. Server: Temp files.....	23
4.8. Server: Server space.....	24
4.9. Server: Send logs	25
4.10. Database: General configuration	25
4.11. Database: Transactions	26
4.12. Database: Index statistics.....	26
4.13. Database: Active users	27
4.14. Database: Backup.....	27
4.15. Database: Store metadata	29

4.16. Database: Validate DB.....	30
4.17. Database: Delta-files monitoring	31
4.18. Database: Disk space.....	31
4.19. Database: Database statistics	32
4.20. Database: Send logs	32
5. FBDataGuard tips&tricks	33
5.1. Path to FBDataGuard configuration	33
5.2. Adjusting web-console port	33
Appendix: CRON Expressions	34
CRON Format.....	34
Special characters.....	34
CRON Examples	35
Notes	36
6. Support contacts	36

Guia do usuário do FBDataGuard for Windows

1. O que é IBSurgeon's FBDataGuard?

FBDataGuard é uma ferramenta server-side para monitorar bancos de dados Firebird e impedir corrupções. Ele observa para bancos de dados e ambiente de servidor, executa backups *in right way*, reúne estatísticas e envia alertas sobre problemas reais e possíveis.

FBDataGuard pretende ser mantenedor automático e assistente de administrador de bancos de dados Firebird importantes, especialmente em locais remotos e ser distribuído com software que utiliza Firebird.

Sobre a IBSurgeon

IBSurgeon (www.ib-aid.com) foi fundada em 2002 com a idéia de fornecer a desenvolvedores e administradores InterBase e Firebird serviços exclusivos e ferramentas focadas em segurança, desempenho e disponibilidade para bancos de dados. IBSurgeon é um patrocinador Platinum da Fundação Firebird e, como membro do Grupo de Trabalho Técnico, tem forte relação com o Projeto Firebird, com representantes diretos no Firebird-Admins e na Comissão da Fundação Firebird. Hoje, IBSurgeon atende mais de 2.000 empresas de todo o mundo com emergências, otimização, ferramentas de manutenção e serviços diversos.



2. Instalação

2.1. Download e registro

Cada instância de FBDataGuard deve ser registrado de acordo com o seu contrato de licença (única exceção é pacote especial para o ISV, projetado para ser instalado e usado como parte de um aplicativo de terceiros, entre em contato isv@ib-aid.com para detalhes).

Como fazer o download do FBDataGuard

- 1) Obtenha a conta para o IBSurgeon Deploy Center, username e senha para efetuar download e ativar os produtos IBSurgeon. Visite: http://ib-aid.com/products/firebird_interbase/protection_tools/IBDataGuard-FBDataGuard para maiores detalhes.
- 2) Eetue o Login no IBSurgeon Deploy Center <http://deploy.ib-aid.com> (ex www.ib-aid.com:8180) com seu username e password e verifique se especificou corretamente seu e-mail – Ele será utilizado para o envio das informações da licença.
- 3) Escolha FBDataGuard na lista de produtos licenciados e escolha o link “Download”, então efetue o **download FBDataGuard**, descompacte-o utilizando a senha que aparece próxima ao nome do arquivo e instale-o.

Como registrar FBDataGuard

Após a instalação do FBDataGuard (observe

- 1) Depois salve o arquivo gerado: license.uik no seu computador
- 2) Logue no IBSurgeon Deploy center: <http://deploy.ib-aid.com> (ex www.ib-aid.com:8180), e escolha o link "Activate"



List of owned products' licenses:

Product name	Description	Downloads	Available activations	Used activations	End license date	Actions
FBDataGuard 2.5	Monitor, recover, protect Firebird database	Download	2	0	2099-12-29	Activate

- 3) Faça o Upload do arquivo license.uik para o IBSurgeon Deploy Center



Create new (1) or use existing activations (2) from list below

1. Create new activation

To activate your application, please upload UIK file, generated by your application's registration wizard

Please select file with your registration information (UIK):

Description (for your purposes)

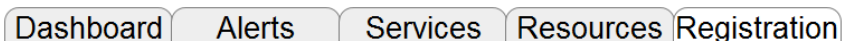
UIK file name:

- 4) Faça o Download do arquivo de destravamento da lista de ativações disponíveis e salve em seu computador. Também sera enviado por e-mail.
- 5) Retorne a tab FBDataGuard, "Registration" e clique em [Upload license file \(*.unlk\) >>](#)
- 6) Escolha fbdg.unlk e o FBDataGuard estará registrado nesse computador.

Nota:

O registro do FBDataGuard registration é baseado em **AgentID**, **network name** e **IP address** do servidor onde o FBDataGuard está instalado. Se isso for modificado, FBDataGuard será modificado para não registrado.

- 7) 2.2. Instalação no Windows) e acrescentado o Firebird Serve para monitorar clique em "Registration" tab no FBDataGuard:



- 8) Escolha o link [Create license request file \(*.uik\) >>](#)

- 9) Digite seu nome, empresa e e-mail. Importante! O e-mail precisa ser o mesmo especificado na conta do IBSurgeon Deploy Center, caso contrário o registro irá falhar:

- 10) Depois salve o arquivo gerado: license.uik no seu computador

- 11) Logue no IBSurgeon Deploy center: <http://deploy.ib-aid.com> (ex www.ib-aid.com:8180), e escolha o link "Activate"



List of owned products' licenses:

Product name	Description	Downloads	Available activations	Used activations	End license date	Actions
FBDataGuard 2.5 Monitor, recover, protect Firebird database		Download 2	0		2099-12-29	Activate

- 12) Faça o Upload do arquivo license.uik para o IBSurgeon Deploy Center



Create new (1) or use existing activations (2) from list below

1. Create new activation

To activate your application, please upload UIK file, generated by your application's registration wizard

Please select file with your registration information (UIK):

Description (for your purposes)

UIK file name:

- 13) Faça o Download do arquivo de destravamento da lista de ativações disponíveis e salve em seu computador. Também sera enviado por e-mail.

- 14) Retorne a tab FBDataGuard, "Registration" e clique em [Upload license file \(*.unlk\) >>](#)

- 15) Escolha fbdg.unlk e o FBDataGuard estará registrado nesse computador.

Nota:

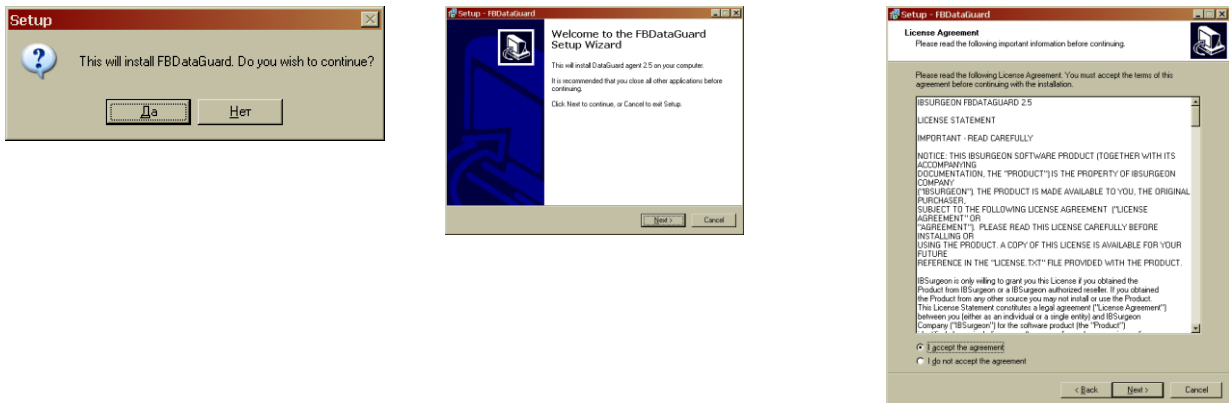
O registro do FBDataGuard registration é baseado em **AgentID, network name e IP address** do servidor onde o FBDataGuard está instalado. Se isso for modificado, FBDataGuard será modificado para não registrado.

2.2. Instalação no Windows

Nessa seção discutimos os processos de instalação do FBDataGuard para Windows.

FBDataGuard deverá ser instalado no mesmo computador onde o Firebird está rodando. Ele não poderá monitorar o servidor Firebird, os bancos de dados e o ambiente de hardware à partir de um computador remoto.

Para instalar o FBDataGuard você precisa iniciar o instalador com direitos de administrador e passar por diversas etapas. Primeiros passos são obviamente: Start, a notificação do que será instalado e a aceitação do acordo de licença.



Então você precisa selecionar a pasta onde instalar FBDataGuard. Por padrão, ele oferece **C: \ Arquivos de Programas \FBDataGuard**. Você pode aceitá-lo ou escolher outro local.

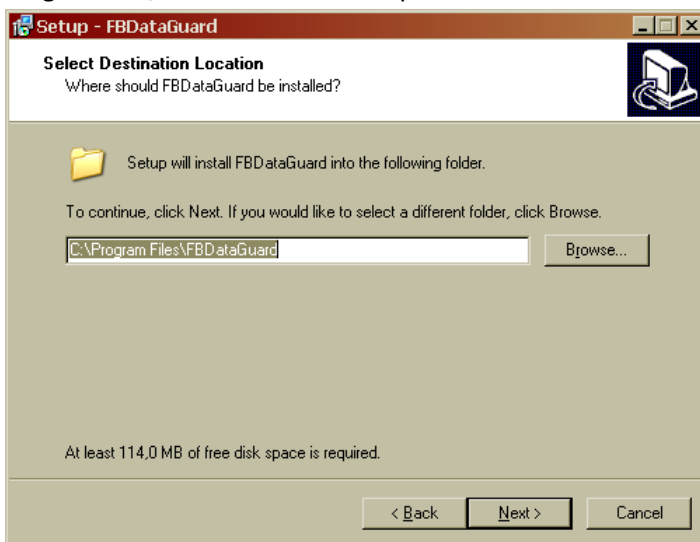


Figura Selecione onde instalar o FBDataGuard

2.3. Escolhendo pastas para armazenar configuração, backups e estatísticas

O próximo passo é importante. O instalador do FBDataGuard precisa saber onde armazenar a configuração do FBDataGuard, backups e estatísticas.

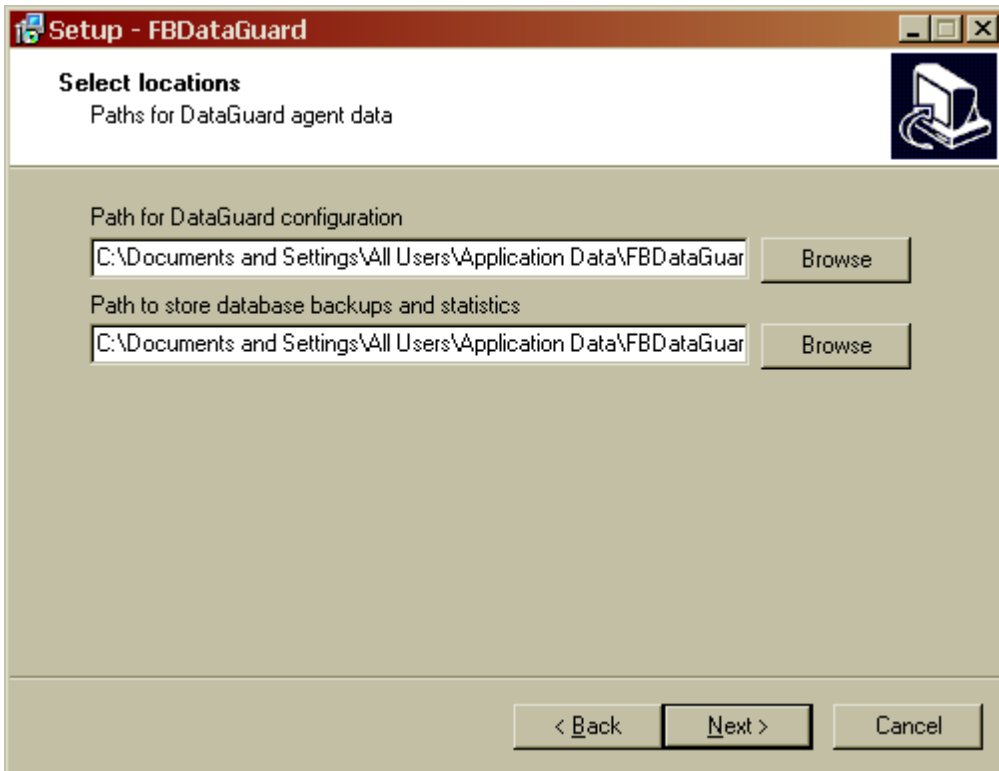


Figura Escolha a pasta para armazenar as configurações backups e estatísticas do FBDataGuard

Recomendamos fortemente que **não use as configurações padrão**. A melhor maneira é apontar configuração e pastas de backup para a unidade local com backups (não mapeados). Por exemplo, se seu banco de dados é colocado no D: \, e backups está em F: \, recomendamos usar algo como:

Path para a configuração do DataGuard

F:\FBDataGuard\config

Path para backups de bancos de dados e estatísticas

F:\mybackups

Você também pode especificar explicitamente mais tarde o caminho para a pasta com o backup, durante a configuração do sistema de monitoramento, mas recomendamos fazê-lo durante a instalação. Pastas para armazenar backups geralmente requerem muito espaço.

Depois disso, você será solicitado para confirmar se você deseja instalar FBDataGuard como um serviço e iniciar tal. Prosseguir com outras etapas de instalação, clicando em "Next" e finalizando. Então, temos de avançar com o FBDataGuard nas configurações iniciais.

2.4. Instalação no Linux

Não há nenhum instalador do FBDataGuard 2.8 para Linux (bem como para Mac OS X). Você precisa efetuar download do arquivo dataguard28.zip (www.ib-aid.com/dgupdates/dataguard28.zip) e seguir as seguintes instruções:

Pre-requisitos

Para todas as versões de Linux, certifique-se que tem direitos de root (su ou sudo):

1) Descompacte este pacote para a pasta apropriada (por exemplo: /opt/dataguard28)

2) Altere o *owner* da pasta dataguard28 para o user *firebird*:

chown -R firebird dataguard28

3) Acrescente as permissões necessárias para execução:

run.sh (Todas as versões de Linux)

dg_debian_run.sh (Debian)

dg_centos.sh (CentOS)

dg_suse.sh (Suse)

4) Instale o Java. Pode ser o Sun (Oracle) Java ou OpenJDK 1.6 e mais atual.

Mais informações: <http://openjdk.java.net/install/>

Comandos para as principais distros:

Ubuntu

\$ sudo apt-get install openjdk-6-jre

OpenSuse

\$ sudo zypper install java-1.6.0-openjdk

Fedora, Red Hat Enterprise Linux, CentOS

\$ su -c "yum install java-1.6.0-openjdk"

(or look for specific OS instructions)

Debian

\$ sudo apt-get install openjdk-6-jre

5) Tente rodar FBDataGuard como uma aplicação (à partir de /opt/dataguard28):

./run.sh

Se o Java estiver instalado corretamente, FBDataGuard pode rodar como aplicação. Observe a saída e feche-a.

Passos para instalação

Os próximos passos são requeridos para rodar FBDataGuard como um serviço. Requer direitos de superusuário (**sudo** or **su**).

Debian

1) instale jsvc service runner (java será instalado como dependência):

\$ sudo apt-get install jsvc

- 2) Verifique se **JAVA_HOME** se está diferente de `/usr/lib/jvm/java-6-openjdk/jre`, indique o local correto (`JAVA_HOME=`) no arquivo **dg_debian_run.sh**
- 3) Indique o local do FBDataGuard para **DG_HOME** (por default é `/opt/dataguard28`)
- 4) Inicie o FBDataGuard à partir da pasta FBDataGuard
./dg_debian_run.sh start
- 5) Por default FBDataGuard monitora localhost – Está acessível apenas localmente (`http://localhost:8082`). Para ativar conexões externas edit o arquivo `/opt/dataguard28/conf/network.properties` e indique o valor do IP em **server.bind-address** (Digite `ifconfig` para descobrir seu IP, `/sbin/ifconfig` no CentOS)

CENTOS

- 1) Instalar service com comando
./dg_centos.sh install
- 2) Rode FBdataGuard service com o comando
./etc/init.d/dataguard28 start

OpenSuse

- 1) Instalar service com o comando
./dg_suse.sh install
- 2) Rode o service com o comando
./etc/init.d/dataguard28 start

Para outras distribuições Linux – use: **dg_centos.sh**.

3. Configuração inicial do FBDataGuard

Depois de instalar FBDataGuard precisamos configurá-lo. Por favor, siga estes passos:

1. Certifique-se de que você tem Firebird 1.5 ou posterior e que está trabalhando;
2. FBDataGuard serviço é instalado e iniciado corretamente. Você pode verificá-lo usando os Serviços de applet em Painel de controle (botão direito do mouse em "Meu Computador", selecione "Gerenciar" e depois em "Serviços e Aplicações", "Serviços" e encontrar na lista "FBDataGuard Agent"
3. Verifique se a porta FBDataGuard é acessível (8082) e não é bloqueada pelo firewall ou quaisquer outras ferramentas antivírus. Se necessário, ajustar a porta na configuração FBDataGuard (ver).

Importante: Em sistemas Windows sem o pacote do Microsoft Visual Studio a carga do software (RunAsAdmin.exe) não vai funcionar, então você precisa executar instalar e desinstalar os scripts (procrun-install e procrun-uninstall) manualmente a partir do prompt de comando lançado com a privilégios de administrador.

3.1. Abrindo o web-console

Para abrir o web console, digite em seu browser: <https://localhost:8082> or <https://127.0.0.1:8082>

Ou você pode escolher "Iniciar" menu FBDataGuard\ "Launch the DataGuard web console for localhost"

Browsers suportados

FBDataGuard web-console pode rodar corretamente com Firefox, Safari e Internet Explorer.

Mensagens de erro com relação ao certificado

Inicialmente o browser apontará para (<https://localhost:8082>) não é seguro, e ele vai recomendar deixar o web-site. Esta mensagem é causada pelo certificado de segurança padrão para FBDataGuard web-console.

Por favor, ignore essa mensagem e clicar para abrir FBDataGuard web-console.

Ele irá pedir o nome de usuário e senha (dialog de login pode ser diferente para Firefox, Safari ou Chrome)

Nome de usuário / senha padrão para web-console é "admin" / "strong password" (sem aspas).

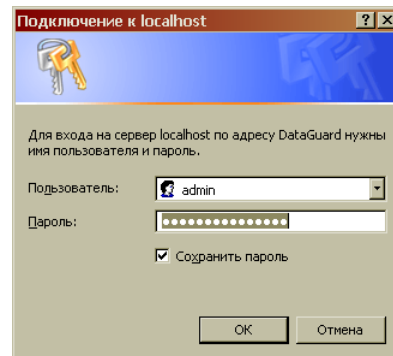


Figura 1 Entre username e password para FBDataGuard web-console

3.2. Recurso de descoberta automática do FBDataGuard

Na primeira execução o FBDataGuard irá checar computadores com Firebird Servers instalados.

FBDataGuard para Windows buscará registros do Firebird no registry, FBDataGuard para Linux and Mac OS X checando os locais padrão de instalação.

FBDataGuard irá mostrar a lista de todos Firebird cópias instaladas, mas apenas a uma instância do Firebird pode ser monitorado por FBDataGuard. Escolha clicando *“Add to monitoring >>”*

Se você não vê instância do Firebird na lista de descoberta automática, você pode escolher *“Add custom >>”* e configurar a instância manualmente.

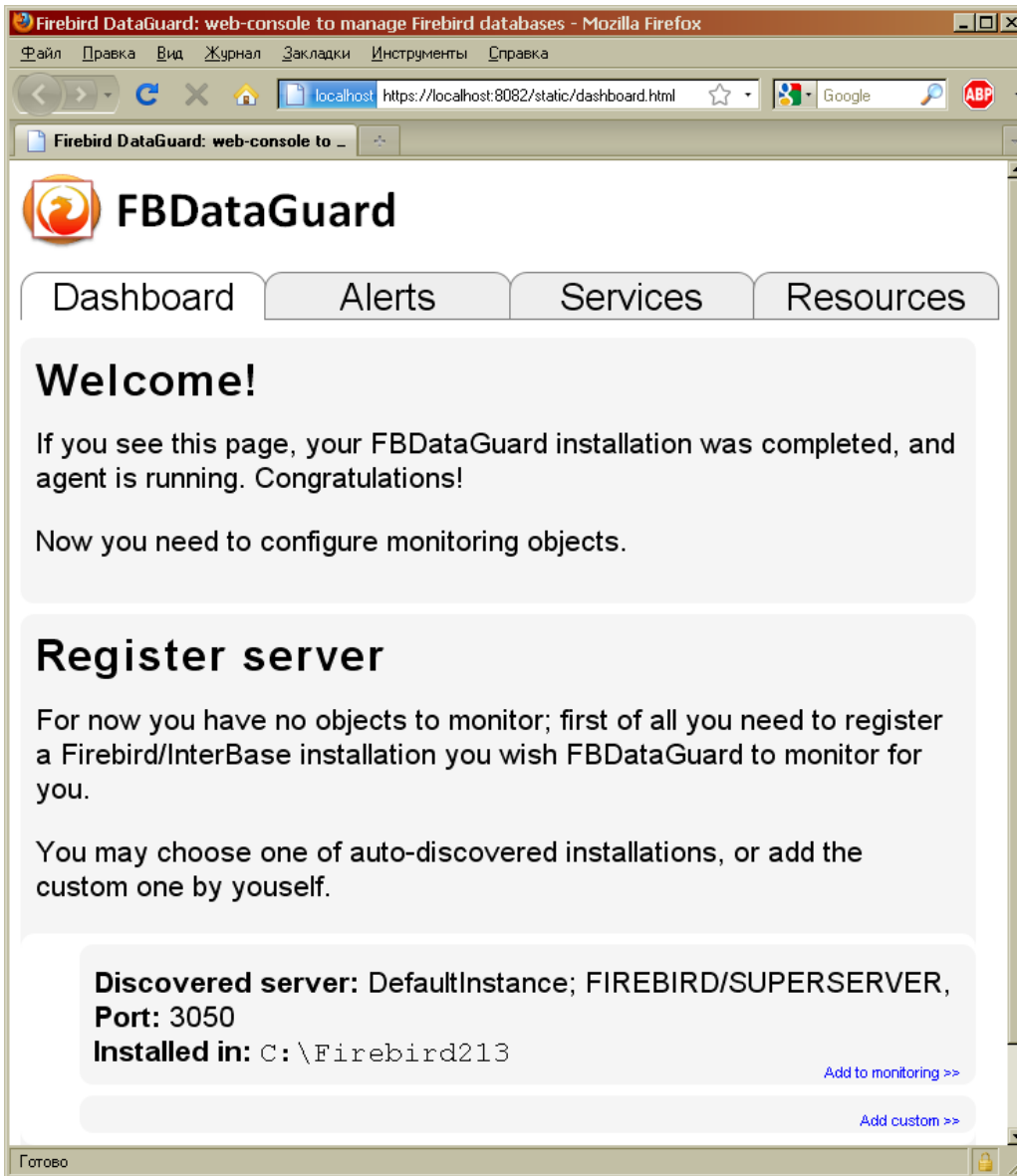


Figura 2 Descoberta automatic no FBDataGuard

3.3. Registrando o Servidor Firebird

Para registrar servidores descobertos você precisa clicar em “Add to monitoring>>” e depois ajuste as configurações de descoberta.

Nota: para usar a autenticação Windows Trusted (por padrão é off) que você precisa ter certeza de que as bibliotecas jaybird21.dll e fbclient.dll (a partir da versão Firebird for o caso) são encontradas nos caminhos do Windows.

FBDataGuard oferece padrões para o Firebird server. Nós encorajamos fortemente alterar o parâmetro “Output directory”.

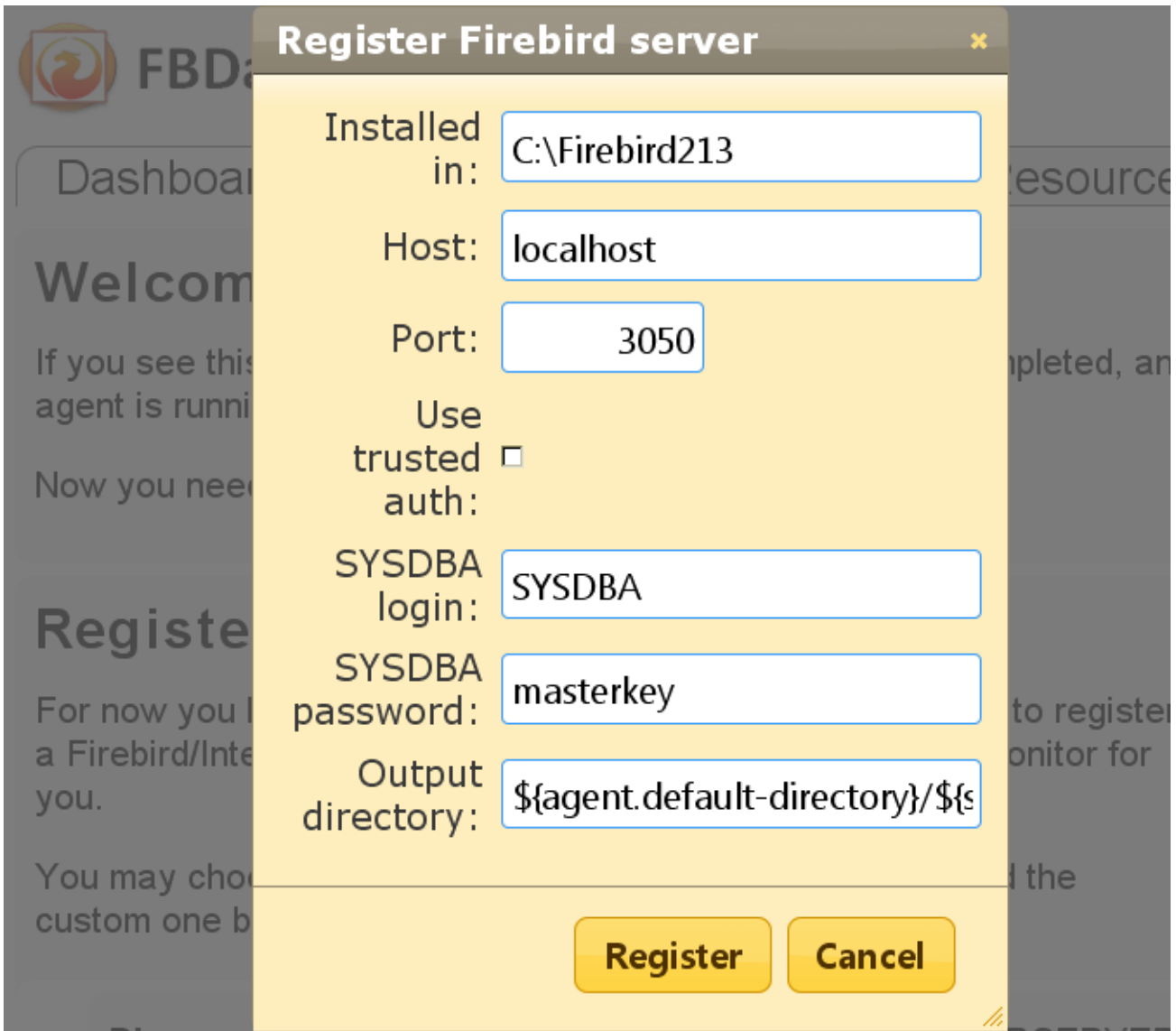


Figura 3 Registrando servidor no FBDataGuard

Por default o “Output directory” para o Firebird server é **`${agent.default-directory}/${server.id}`**

Isso significa que os backups, estatísticas e registros recolhidos serão armazenados na pasta de backups especificados em []. Ele pode não ser muito conveniente, por isso, recomendado que aponte o diretório de saída do FBDataGuard para um caminho mais simples, geralmente situado no disco, por exemplo

F:\myserverdata

Depois que clicar em “Register” FBDataGuard será populado por padrão com arquivos de configurações e iniciará imediatamente a análise do firebird.log. Pode demorar um tempo (por exemplo, 1 minuto para 60Mb firebird.log). Depois você vai ver primeiro na web-console o servidor Firebird registrado:

Firebird DataGuard - ©IBSurgeon, 2008-2010 - Firebird SQL web site

Figure 4 Web-console com servidor Firebird registrado

FBDataGuard mostra alertas e status de objetos monitorados. Como você pode ver, neste exemplo FBDataGuard encontrou mensagens de erro no firebird. Log e determinou que o tamanho da instalação do servidor Firebird é muito grande. Vamos considerar em detalhes cada um dos objetos monitorados e suas configurações.

Nota: Você não pode excluir um servidor Firebird registrado no em FBDataGuard 2.8 pela web-console do Centro de Controle. A única maneira de cancelar o registro do servidor é apagar seus arquivos de configuração. Em geral, não há nenhuma razão para exclusão de um servidor registrado, até que você queira desinstalar completamente FBDataGuard.

Agora precisamos prosseguir com o registro de banco de dados.

3.4. Registrando o banco de dados Firebird

Para registrar um banco de dados no FBDataGuard, você precisa clicar em “Add database to monitoring>>” e preencher o seguinte formulário:

Database monitoring configuration: 9d58e402-af24-41eb-a1ef-58f2101f1390

Database name:

DB alias:

Path to database:

Output directory:

Save **Cancel**

No cabeçalho do formulário você verá o GUID do banco de dados - é usado para identificação única de banco de dados. Ele é usado apenas internamente, não há necessidade de se lembrar.

“**Database name**” é por conveniência ao se referir banco de dados em mensagens e alertas de e-mail.

“**DB alias**” é um alias de banco de dados, do `aliases.conf`. Se você especificar “DB Alias” e “Path to database”, “DB Alias” será usado.

“**Path to database**” é o caminho para o banco de dados (lembre-se que o FBDataGuard poderia rodar no mesmo computador onde está o Firebird). Se você colocar o banco de dados em um drive externo, isso pode provocar um “File... has unknown partition”. Para corrigir clique em “Configure” no widget do servidor e clique em “Save” para forçar FBDataGuard reler as partições.

“**Output directory**” é o folder onde FBDataGuard irá armazenar seu banco de dados de backups, logs e estatísticas. É uma boa idéia especificar “Output directory” Para uma localização explícita como `F:\mydatabasedata`

Nota: você pode especificar locais absolutos para backups e estatísticas posteriormente em através de dialogs (observe que após o registro o FBDataGuard irá popular o banco de dados de configuração com valores default e mostrar na web-console com o banco de dados registrado:

*

Figure 5 FBDataGuard web-console com os bancos de dados

Você pode ajustar as configurações de banco de dados posteriormente; agora vamos configurar os alertas.

3.5. Alerta de email no FBDataGuard

FBDataGuard pode enviar alertas para os administradores que contêm informações sobre backups de sucesso e os problemas potenciais e reais com bancos de dados.

É uma idéia muito boa para configurar o envio por correio eletrônico de alertas. Para fazer isso você precisa clicar na ligação “Configure” na frente de “Alerts” na seção Web-console.



Alerts configuration ✕

Installation name:

Installation GUID:

Raise warning for suspicious backup paths:

Sent alerts by e-mail:

Anti-spam delay, min:

Send alerts to:

'From' field:

SMTP server address:

SMTP server port:

Secure (SSL) connection:

SMTP server login:

SMTP server password:

Save **Cancel**

Figure 6 Janela de configuração de alertas por e-mail do FBDataGuard

Primeiro de tudo, você precisa habilitar o envio de alertas ativando o checkbox **“Send alerts by e-mail”**. **“Installation name”** é o nome legível para sua conveniência, ele vai ser encaminhado em e-mails e alertas. **“Installation GUID”** é um campo de service, não há necessidade de alterá-lo. **“Raise warning for suspicious backup paths”** é para avisar sobre o arquivo de backup potencialmente errado, por exemplo, se o banco de dados é armazenado em "Documents and Settings" ou o comprimento do caminho de backup é muito longo. **“Anti-spam delay”** especifica atraso no envio de mensagens repetidas. Ele evita a inundação da caixa de correio dos administradores com mensagens repetitivas. 60 minutos é um valor ideal. **“Send alerts to”** especifica para onde serão enviados os e-mails. **“From field”** É o que será colocado como remetente no e-mail. **“SMTP server address”, “SMTP server port”, “SMTP server login” e “SMTP server password”** São dados que serão usados nos e-mails. Clique **“Save”** Para salvar a configuração de alertas. *Não pode haver atraso ao salvar, já que FBDataGuard está verificando as configurações e envia e-mail de teste para o endereço especificado.*

3.6. Próximos passos com FBDataGuard

Depois de ter o FBDataGuard configurado e acrescentado que servidor e banco de dados devem ser monitorados, você precisa ajustar as configurações para as atividades de manutenção mais importantes: backup e Atividades de monitoramento de espaço. Outros podem ser configurados mais tarde.

Por favor agora vá a seção [4.14. Database: Backup](#), [4.8. Server: Server space](#) e [4.18. Database:](#) para obter maiores informações.

3.7. Embuta FBDataGuard dentro de suas aplicações

É fácil incorporar FBDataGuard em sua própria aplicação, que será instalado silenciosamente e vai assistir a seu banco de dados.

Se você é um vendedor de aplicação banco de dados baseado em Firebird e precisa saber como incorporar FBDataGuard no pacote de instalação do seu aplicativo (por favor, note que licença especial é necessária para a agregação FBDataGuard com suas aplicações) entre em contato IBSurgeon em dg@ib-aid.com e iremos fornecer-lhe todas as informações necessárias.

4. Configurando a web console do FBDataGuard

4.1. Resumo da Web-console

Partes da web-console

A Web-console do FBDataGuard contém 4 tabs: Dashboard, Alerts, Services e Resources. “Dashboard” é a principal tab onde o administrador pode configurar o FBDataGuard e visualizar os status dos servidores. “Alerts” contém uma lista completa de alertas gerados pelo FBDataGuard. “Services” contém links para outros services da IBSurgeon (a lista de services expandirá), e “Resources” - links recursos externos úteis.



Jobs

FBDataGuard web-console destina-se a facilitar a edição de configurações de atividades (chamados de "jobs"), que são executadas pelo FBDataGuard (nem todos os jobs estão listados no web-console, alguns deles estão disponíveis somente através de edição direta de arquivos de configuração).

Quase todos os trabalhos FBDataGuard tem duas finalidades: a primeira é para monitorar algum valor e gerar alertas, se necessário, e a segunda é a de armazenar os valores históricos em logs, para mais tarde analisar a dinâmica de todos os parâmetros do servidor Firebird e banco de dados.

Nesta seção, vamos considerar a configuração geral dos parâmetros dos jobs, mas não uma análise de log reunidos.

Jobs widgets

É o seguinte: cada atividade é representada por um "widget", que tem as seguintes partes:

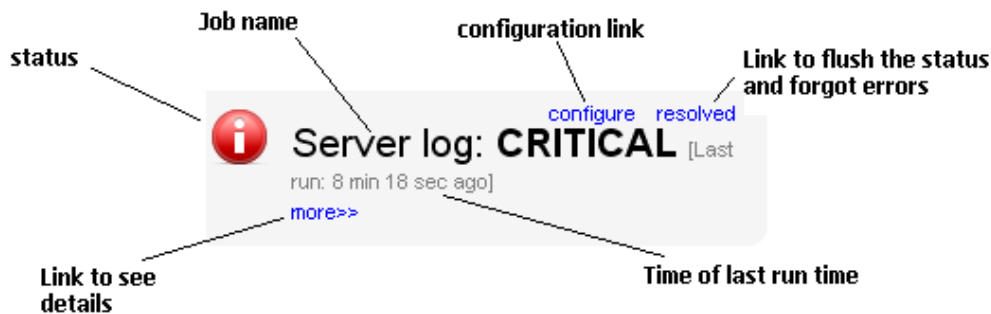


Figure 7 Elementos dos widgets do web-console do FBDataGuard

Status – indica-se com o ícone de cor e nome. Situação do banco de dados é um resumo de todos os trabalhos em nível do servidor incluídos e status do bancos de dados, e, respectivamente, o estado do banco de dados é um resumo de todos os jobs de níveis de banco de dados.

Status types

CRITICAL significa problemas, **OK** significa “Tudo está ótimo”, **WARNING** significa que algumas questões requerem atenção, **MAJOR** significa questões maiores, **MINOR** – questões menores, **MALFUNCTION** significa que o job não obteve sucesso (alguma coisa segurou sua execução), **NOT_AVAILABLE** significa que aquele job não está disponível naquela versão de servidor de banco de dados.

OFF significa que o job não está ativo, **UNKNOWN** significa que o job não foi iniciado ainda, então os resultados são desconhecidos.

Job name indica no nome da atividade.

Configuration link abre o diálogo de configuração, que é individual para cada job.

Resolved é o link para desativar o status de UNKNOWN e esquecer erros que foram descobertos previamente. O status será atualizado respeitando a corrent situação depois da próxima execução do job.

Last run mostra que o job foi executado pela ultima vez.

More>> é o link que abre o widget e mostra mais detalhes e sugeri medidas para o administrador para resolver a situação.

Outras ligações podem ser associados a banco de dados

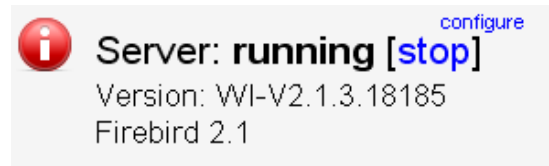
Todos os trabalhos em FBDataGuard têm configurações padrão que são muito próximos dos valores recomendados para a 80% das instalações do Firebird, então depois de servidor de configuração inicial e banco de dados serão protegidos em muito bom nível comparando com a instalação padrão, mas de qualquer maneira recomendamos configuração adicional e ajuste para cada trabalho.

Nas próximas seções, vamos considerar cada job e sua configuração.

4.2. Server: Configuração geral

Server: Widget de configuração geral mostra o status resumido de todos os jobs em nível de servidor e status de bancos de dados monitorados.

Server: General configuration também indica Firebird sendo executado ou não, e fornece links para Stop / Start para cada job Firebird (e único serviço - não afeta Firebird que está sendo executado como aplicativo).



Importante: Tenha cuidado ao usar a funcionalidade Start / Stop do FBDataGuard. Você pode facilmente baixar um servidor Firebird que realiza um trabalho importante.

Se você clicar no link **configure**, vamos ver o mesmo diálogo que temos usado para registrar instância do Firebird no FBDataGuard, e agora ele pode ser usado para mudar propriedades da instância do Firebird:

A longa série de letras e números é o número GUID exclusivo deste servidor Firebird monitorado.

4.3. Server: atualizações automáticas

Atualização automática é uma tarefa importante, avisa que a versão mais recente do FBDataGuard está disponível e se oferece para atualizar o software. Ele fornece um alerta a respeito de atualizações disponíveis e baixar o tempo de link. A hora padrão para executar este trabalho é 22-00 todos os dias (para informações).

No diálogo de configuração de atualizações automáticas, você pode desativar a verificação automática ou definir outro momento para fazê-la.

Para mais informações sobre o formato da hora por favor consulte [Apêndice: expressões do CRON](#)

De fato, há uma pequena confusão aqui: atualização automática não executa a atualização automática de software, ele apenas verifica as novas versões periodicamente.

4.4. Server: Agent Space

Monitoramento de Agent space é destinado para assistir espaço ocupado por registros, estatísticas, repositório de metadados e outros dados, recolhidos pelo FBDataGuard. Para bancos de dados não assistidos por um longo período de tempo (1-2 anos), é possível que os logs FBDataGuard ocupem muito espaço e falta de espaço pode levar a uma falha na base de dados. Para evitar isso, com certeza, Espaço Agent deve estar assistindo para o espaço ocupado.

Por default: Agente trabalho espaço é ativado.

Além disso, se alguém tem ignorado recomendações para colocar as pastas dos backups para as posições explícitas, é possível que o backup do banco de dados seja criado dentro da pasta Agent. Neste caso, você vai ver o status CRITIC imediatamente - FBDataGuard irá reconhecer e avisá-lo sobre a configuração errada.

E, este trabalho é útil para pacotes de FBDataGuard e aplicativos de terceiros.

Na caixa de diálogo de configuração, você pode ativar / desativar este trabalho, definir período de verificação (por padrão é 10 minutos), e definir limites para alertas.

Os limites podem ser definidos em% do tamanho máximo ocupado pelo registro ou usando o tamanho explícito em bytes.

FBDataGuard verifica os valores e levanta alerta para o primeiro limite. Se você quiser definir somente%, você precisa definir -1 como valor de "Max occupied".

4.5. Server: Server version

FBDataGuard verifica a versão do servidor Firebird. Se a versão não está na lista de servidores suportados dá um aviso.

É tarefa muito simples, porém útil em alguns casos empregos: ele vai garantir que o usuário de aplicativo baseado Firebird está trabalhando com a versão recomendada.

A versão atual do FBDataGuard suporta 1.5.x, 2.5.x

4.6. Server: Server log

"Server log" é um dos trabalhos mais sofisticados FBDataGuard a partir do ponto de vista de suas características e implementações, mas é tão fácil de configurar como outros trabalhos são.

Este trabalho verifica periodicamente firebird.log e se ele detecta esse arquivo foi alterado, log inicia análise. Motor analítico embutido verifica cada entrada no firebird.log e classificá-lo em várias categorias, com diferentes níveis de gravidade.

De acordo com a gravidade do quadro de mensagens de trabalho é atribuído e alertas apropriados são gerados.

Uma vez administrador reviu erros e alertas (e executou ações necessárias para resolver o motivo do erro), ele clica no link "resolvido" e FBDataGuard vai esquecer as mensagens de erro antigas no firebird.log.

Na configuração de "log do servidor", você pode ativar / desativar este trabalho e definir o período de retenção (em minutos).

Além disso, este relógio de trabalho para o tamanho do firebird.log e se o tamanho exceder "Tamanho para rolar", FBDataGuard irá dividir firebird.log, registrar e renomeá-lo de acordo com a data padrão.

Parâmetro "Últimos mensagens de erro para armazenar" especifica quantas mensagens de erro mais recentes serão armazenados.

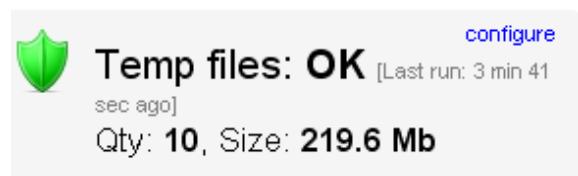
4.7. Server: Temp files

Na configuração de "log do servidor", você pode ativar / desativar este trabalho e definir o período de retenção (em minutos).

Além disso, este relógio de trabalho para o tamanho do firebird.log e se o tamanho exceder "Tamanho para rolar", FBDataGuard irá dividir o firebird.log, registrar e renomeá-lo de acordo com a data padrão. Parâmetro "Últimas mensagens de erro para armazenadas" especifica que "Servidor: arquivos temporários". O trabalho é muito útil para pegar e resolver problemas de desempenho e falhas com banco de dados Firebird.

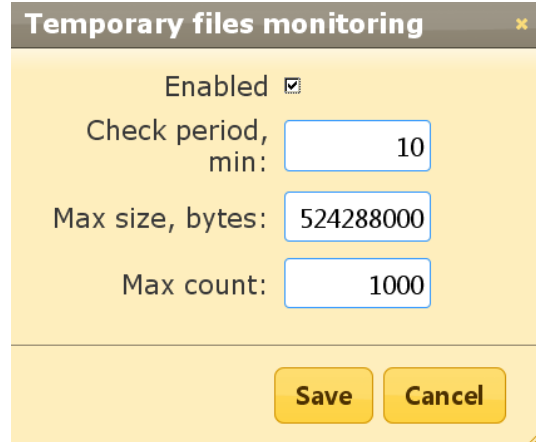
Durante a execução de queries SQL no Firebird os resultados intermediários podem classificar e mesclar fluxos de dados em arquivos temporários, que são alocados em locais especificados (TEMP) e as mensagens de erro mais recentes serão armazenadas lá.

FBDataGuard mostra em "Server: Temp files" Widget informações sobre a quantidade e o tamanho dos arquivos temporários.



FBDataGuard reconhece locais das pastas TEMP e quantidade e o tamanho dos arquivos temporários monitorados. Falta de espaço pode levar ao problema de desempenho ou erros mais graves, muitos (ou muito grande) os arquivos temporários podem indicar problemas com a qualidade das queries SQL.

Usando o diálogo de configuração, você pode ativar / desativar este trabalho, definir o período e os limites para o tamanho máximo de arquivos temporários (o tamanho de todos os arquivos) e quantidade.



Temporary files monitoring ✕

Enabled

Check period, min:

Max size, bytes:

Max count:

Save Cancel

4.8. Server: Server space

Os jobs de “Server space” monitor o tamanho da instalação ocupada pelo Firebird server. É ativado por default.

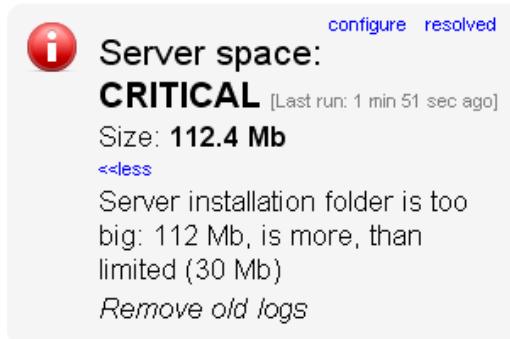
Existem várias ameaças evitadas por este job: questões de má administração quando os volumes de banco de dados ou tabelas externas estão sendo criados em %Firebird%\Bin, **firebird.log** muito grandes que pode esgotar todo espaço do drive com a instalação do Firebird, e alguns outros problemas.

Além disso, este job monitora e analisa as informações, recolhidas por todos os trabalhos relacionados com o espaço (incluindo empregos de nível de banco de dados).

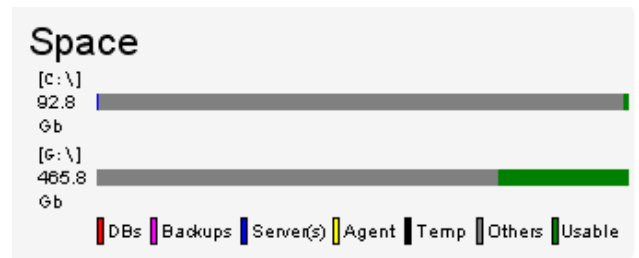
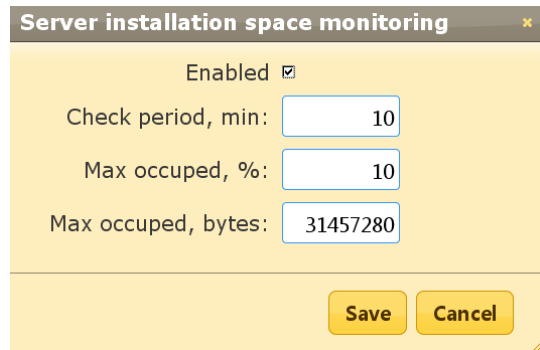
Na imagem ao lado você pode ver a representação rápida de análise espacial para todas as unidades onde Firebird, bases de dados e backups serão armazenados.

Usando o diálogo de configuração, você pode ativar / desativar esse trabalho, determinado período de verificação e limites para o tamanho da pasta do servidor.

Por padrão, usamos 30Mb é uma definição padrão para a instalação do Firebird. Se o tamanho do seu Firebird é maior, por favor considere a limpeza de registros antigos e outras informações indesejadas.



Server space: [configure](#) [resolved](#)
CRITICAL [Last run: 1 min 51 sec ago]
 Size: **112.4 Mb**
[<<less](#)
 Server installation folder is too big: 112 Mb, is more, than limited (30 Mb)
Remove old logs

Server installation space monitoring ✕

Enabled

Check period, min:

Max occupied, %:

Max occupied, bytes:

Save Cancel

4.9. Server: Send logs

“Send logs” é um job auxiliar que envia os logs de jobs a nível de servidor por e-mail com a frequência desejada. Este trabalho é desativado por padrão.

Se o banco de dados monitorado está situado em local remoto é útil para agendar o envio de registros por e-mail. Usando o diálogo de configuração, você pode agendar o envio de registros de expressões do

CRON (para maiores detalhes veja [Apêndice: expressões do CRON](#)), especifique para que e-mail será enviado.

Send database logs

Enabled

Schedule: 0 0 23 ? * MON-FRI

E-mail from: dataguard@here.com

E-mail to: whoami@whereami.com

Jobs ids: check-server-log, check-server-space, check-server-running

Save Cancel

Além disso, você pode especificar os logs a serem enviados, especificando os respectivos IDs.

4.10. Database: General configuration

FBDataGuard pode monitorar vários bancos de dados em um único servidor.

Para cada banco de dados é criado um widget separado. No estado de banco de dados top widget é mostrado, apelido de banco de dados (que é especificado durante a adição de dados e pode ser alterado). Também Widget de banco de dados mostra o caminho completo para o banco de dados, seu tamanho e estado de backups.

Link more >> expande os jobs para este banco de dados (ver próximas seções para trabalhos descrições de nível de banco de dados).

test1: OK [configure](#) [remove](#)

G:\databasew\test21_2.FDB

Size: 84.6 Mb

Backups: Ok [more>>](#)

[add database](#)

Usando o diálogo de configuração você pode definir apelido para os bancos de dados, caminho para o banco de dados e o diretório de saída.

FBDataGuard verifica a validade de caminho ao banco de dados e não permite informar caminho errado.

No título do diálogo, você pode ver GUID deste banco de dados monitorado, é usado para identificação única de banco de dados e registros relacionados.

Database monitoring configuration:
976ed805-4fd8-42c4-8236-726a8677ba1f

Database name: test1

Path to database: G:\databasew\test21_2.FDB

Output directory: \${server.default-directory}\\${db.id}

Save Cancel

4.11. Database: Transactions

O job de "Database: Transactions" registra a atividade de transações. Mais tarde, esses registros podem ser analisados para se obter uma visão útil sobre o desempenho do banco de dados e a qualidade da aplicação (ver mais informações aqui <http://www.ibm-aid.com/articles/item66>).

Além disso, este trabalho de monitoriza o limite de aplicação no Firebird: número máximo de transações deve ser inferior a $2^{32}-1$. Junto a este banco de dados número deve ser backup e restaurado.

Ele vai lançar um alerta se o número de transação estiver próximo das restrições.

4.12. Database: Index statistics

"Database: Index statistics" é um job muito importante que está relacionada não só com os índices e seu desempenho, mas também verificar se há corrupção.

"Database: index statistics" Permite executar re-computação de valor de seletividade do índice. Durante este procedimento o Firebird rapidamente percorre as páginas de índices e renova as estatísticas sobre a sua seletividade. Ao visitar estas páginas Firebird também verifica a sua integridade e se o índice está corrompido, um aviso será gerado.

Além disso, este trabalho verifica-se que todos os índices são ativos no banco de dados. Índices inativos ou não ativados geralmente indicam a corrupção e levar à degradação de desempenho.

Por default este job é desabilitado, mas recomendamos para habilitá-lo após a seleção cuidadosa dos índices.

Existem 3 modos para esse job: AUTO, ALL e SELECTED.

ALL é o modo onde todos os links serão checados.

AUTO é o modo default. Ele é muito similar ao ALL, mas também verifica o tamanho da base de dados e não afetam os índices de dados, se for maior do que 3,6 GB.

SELECTED é o modo recomendado. Ele permite a escolha de índices que devem ser aferidas ou aqueles que devem ser evitados. Para incluir

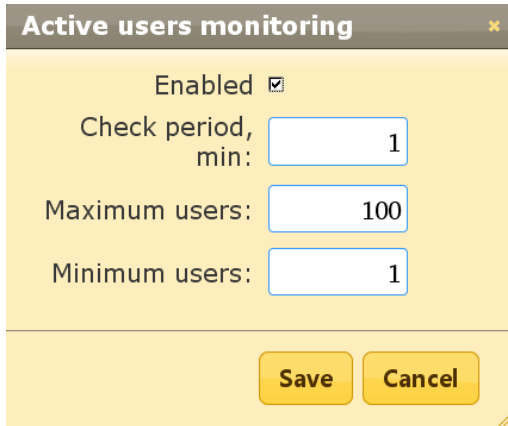
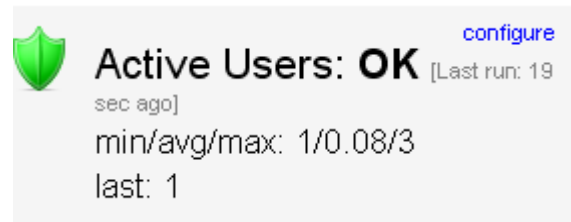
Índices na lista de recomputed, você precisa especificar nomes de índices (dividido por vírgula), e para excluir - executar a mesma.

Como você pode ver a configuração de tela de diálogo, existe campos para ativar / desativar trabalho, para definir o modo de atualização, e para incluir ou excluir índices. "DB tamanho para mudar, bytes" é para definir o limite em que o modo AUTO está funcionando. "Verificar índice de atividade" deve ser sempre ligado, até que você não está realizando manipulações especiais com índices de inativos.

4.13. Database: Active users

“Database: Active users” checa para o número de usuários ativos e calcula mínimos usuários, máxima e média dos usuários e também armazena a atividade dos usuários nos registros de tempo, por isso é possível ver qual era a situação com conexões em determinado período de tempo.

Como você pode ver no widget do job, “Database: Active users” cheques mostra o número mínimo, médio e máximo para o período das últimas 24 horas.

Há limites para o número mínimo e máximo de usuários. Se o seu banco de dados deve sempre ter em uma lista (ou N) conexões (por exemplo, pode ser algum equipamento automático), você pode definir a contagem mínima do usuário que você espera, e obter aviso quando os usuários contam será menor do que o especificado.

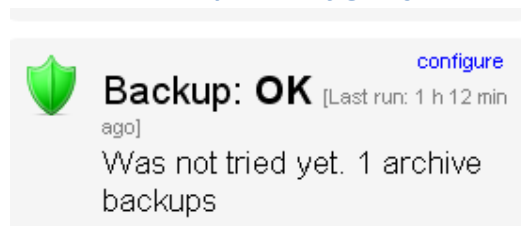
A mesma abordagem é para limite para o número máximo de usuários conectados: por exemplo, para pegar conexões em horários de pico.

4.14. Database: Backup

“Database: Backup” é uma das tarefas principais para garantir a segurança de dados armazenados no banco de dados protegido. Durante o desenvolvimento de FBDataGuard que tínhamos em mente cenário de recuperação de certo, e este cenário implica que o objetivo fundamental de proteção do banco de dados é a de minimizar as perdas de dados. Se tivermos apoio saudável, a recuperação pode ser concentrada apenas com os dados mais recentes (só o que entrou no banco de dados), e diminuir significativamente o tempo de interrupção geral.

Como você verá abaixo, “Database: Backup” não é apenas um wrapper para a funcionalidade gbk padrão e programador, este é um trabalho inteligente, que tem um monte construído em regras para evitar quaisquer problemas com backups e fornecer interface adequada para gerenciar backup.

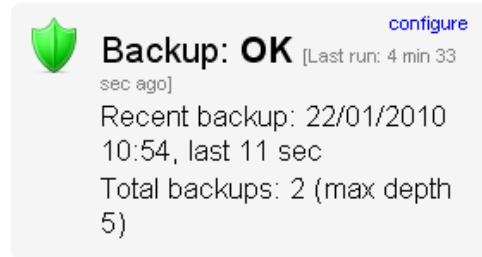
“Database: Backup é ativado por padrão, mas recomendamos fortemente a revisão de sua configuração imediatamente após a configuração do FBDataGuard.



Inicialmente “Database: Backup” é mostrado como OK, apesar de backup não tenha sido processado. Neste caso OK significa que, pelo menos, que o backup está programado.

Além disso, este trabalho reconhece arquivos de acordo com o padrão de nome (veja abaixo informações sobre a

configuração), e mostra o número total de backups. Depois que o backup foi feito, a informação do Widget será alterado: o tempo de criação do último backup exitosa será mostrado, e também o tempo levou para realmente executar o backup (apenas 11 segundo para a tela com exemplo).



“Database: Backup” verifica o espaço livre no drive com o destino do backup, e se ele detecta que não tenha espaço livre em disco suficiente, um alerta crítico será enviado, e o backup atual será cancelado (se necessário).

Tenha cuidado – por default o backup padrão é agendado para 23-00 Segunda-Sexta. Por default bancos de dados serão armazenados dentro do folder que você especificou durante a instalação!

É muito importante analisar cuidadosamente as definições de backups de banco de dados padrão e ajustá-los de acordo com a configuração local!

The image shows a "Backups configuration" dialog box with the following settings:

- Enabled:
- Schedule: 0 0 23 ? * MON-FRI
- Max duration, min: 120
- Backups into: \${db.default-directory}/\${job.id}
- Backups archive depth: 5
- Backup name pattern: backup_{0,date,yyyyMMdd_HH-mm}
- Backup extension: .fbk
- Compress backups:
- ... with extension: .zbk
- Check restore:
- Restore to: \${backup-directory}/restore.fdb.tmp
- Remove restored:
- Copy backup:
- Copy backup to: /mnt/backups
- Execute shell command:
- Shell command: (empty text box)
- Send 'ok' report:

Buttons: Save, Cancel

No diálogo de configuração do campo “Schedule”, você pode definir o tempo de quando o backup deve ser executado. Scheduler usa expressão CRON e este é um lugar certo para aplicar todo o poder do CRON (veja o [Apêndice: expressões do CRON](#)).

“Max duration” é o período de tempo limite para backup. Às vezes, o processo de backup pode pendurar-se, portanto, superior a do tempo máximo notificará imediatamente administrador de alguns problemas. Além disso, se o backup teve muito tempo, pode significar problemas com a coleta de lixo ou crescimento anormal do próprio banco de dados.

“Backups into” especifica a pasta para armazenar os backups. Esta pasta deve estar no mesmo computador onde o banco de dados está. Por padrão, ele está situado dentro do diretório padrão de banco de dados. Geralmente é uma boa idéia para definir o caminho explícito para as pastas com backups.

“Backups archive depth” especifica quantos backups anteriores deve ser armazenado. Lojas FBDataGuard backups em ordem revólver: quando a profundidade arquivo será alcançado (ou seja, 5 backups será criado), FBDataGuard irá apagar o backup mais antigo e criar um novo backup. Em combinação com expressões CRON dá uma habilidade poderosa para criar a história necessária de backups.

“Backup name pattern” especifica como os arquivos

de backup serão nomeados. Além disso, este padrão de nome permite FBDataGuard reconhecer backups antigos com o same name pattern.

“**Backup extension**” é fbk por default.

“**Compress backups**” especifica deve comprimir os backups do FBDataGuard após backup regular Firebird. Por padrão, esta opção está ligada, mas você precisa saber que FBDataGuard vai fechar os arquivos dos backups que são menos do que 4 GB de tamanho. Após essa compressão serão desligados automaticamente. Recomendamos para ativar esse recurso para pequenos bancos de dados ou banco de dados que funciona em servidores não-dedicados (ou seja, que vem com aplicativos de desktop, por exemplo).

“**...with extension**” Especifica a extensão para arquivos de backup.

“**Check restore**” é um parâmetro muito importante. Se ele estiver em ativo (por padrão), FBDataGuard irá realizar teste de restauração de um backup de novo, a fim de testar a sua validade. Ele garante a qualidade dos backups criados e notificar administrador em caso de eventuais problemas com a restauração de teste.

“**Restore to**” especifica a pasta onde executar uma restauração de teste. Por padrão, ele está dentro de pasta de saída de dados. É uma boa idéia para definir o caminho explícito para o teste de restauração.

“**Remove restored**” specifies should FBDataGuard delete restored database. *Por default é OFF*, assim você pode querer ligá-lo, mas você precisa considerar com cuidado - você realmente precisa para manter a cópia do banco de dados restaurado teste. Com restaurar cada teste esta cópia será substituída.

Opção “**Copy backup**” e “**Copy backup to**” path. Se você tiver local de rede ou drive USB conectado para armazenar banco de dados onde você deseja armazenar cópia de backup (além de backups habituais), FBDataGuard pode copiar o backup mais recente lá: basta ligar o interruptor “cópia de segurança” e especifique o path “**Copy backup to**”.

Opção “**Execute shell command**” e “**Shell command**”. É possível especificar o script personalizado ou executável após o procedimento de backup geral será completa. Shell comando obtém como o caminho para o backup do banco de dados atualizados como parâmetro.

“**Send “Ok” report**” – Por default é off, mas é altamente recomendável para ligá-lo e começar a receber notificações sobre backups corretos. Este recurso irá usar as configurações de e-mail do sistema de alertas (veja [3.5. Alerta de email no FBDataGuard](#)).

4.15. Database: Store metadata

“Database: Store metadata” é uma das tarefas-chave, que garante a proteção de dados em nível baixo. Primeiro de tudo, este trabalho armazena no repositório de metadados matéria especial, portanto, em caso de corrupção pesada de dados, podemos usar o repositório

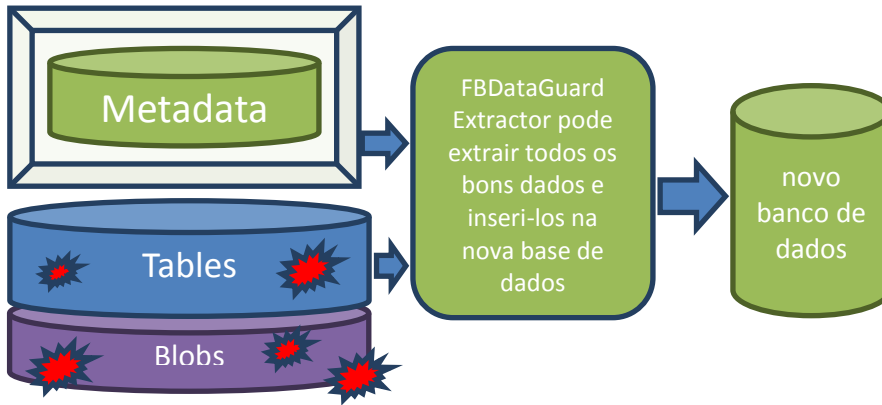


Figure 8 FBDataGuard Extractor pode extrair dados de bancos danificados severamente

O segundo objetivo deste trabalho é verificar constantemente as tabelas para a consistência. A cada 20 minutos ele pinga todas as tabelas no banco de dados e garante que não há erros em nível de metadados. O terceiro objetivo é alertar administrador sobre muitos formatos para cada tabela.

Há um limite de 256 formatos por tabela, mas até mesmo vários formatos podem aumentar consideravelmente chances de corrupção do disco e pode diminuir o desempenho. Recomenda-se não alterar a estrutura das tabelas do banco de dados de produção e manter apenas um formato para cada mesa. Se não for possível, o administrador deve tentar realizar backup / restauração com mais frequência para transformar todos os formatos para o único.

Database metadata backup configuration

Enabled

Check period, min:

Store metadata in:

Date format for folder name:

Folder name prefix:

Max formats:

4.16. Database: Validate DB

Validação de dados Firebird requer acesso exclusivo, ou seja, nenhum usuário deve ser conectado durante a validação. "Banco de dados: Validar DB" fecha o banco de dados e executa a validação do banco de dados e transformá-lo.

Por padrão, esse trabalho é OFF. Por favor, considere cuidadosamente, é possível fornecer acesso exclusivo para banco de dados. A validação também pode levar um tempo significativo. Usando o diálogo de configuração, você pode ativar / desativar este trabalho, definir o tempo a

Update validation configuration

Enabled

Schedule:

Shutdown timeout, sec:

Shutdown mode:

correr, definir o tempo limite de desligamento (tempo de espera antes da validação de lançamento), e também

shutdown mode (FORCE, ATTACH, TRANSACTIONAL). Se você não tem conhecimento profundo do que está fazendo, é melhor manter os parâmetros padrão.

"Database: Validate DB" enviará alerta e colocar dados para o modo crítico se haverá quaisquer erros. Também é possível que esses erros vão ser escrito no firebird.log, então o job agirá em conformidade..

4.17. Database: Monitoranfo Delta-files

Se você estiver usando nBackup, este trabalho é extremamente importante. Ele observa a vida dos delta-files e seu tamanho, e avisa se algo der errado. Esquecer-se dos delta-files são a razão muitas vezes de corrupções e perdas significativas de dados.

Este job encontra todos os arquivos delta associados com banco de dados e verificar a sua idade e tamanho. Se um desses parâmetros exceder os limites "Maximum delta size" ou "maximum delta age", o administrador vai receber o alerta e estado de banco de dados será definido como CRÍTICA.

Nota: Se o arquivo delta do banco de dados protegido foi corrompido, é possível extrair dados a partir dele usando metadata recolhidas.

4.18. Database: Espaço em disco

Este relógios de jobs para todos os objetos relacionados com o banco de dados: arquivos de banco de dados (incluindo volumes de dados multi-volume), deltas, arquivos de backup e assim por diante.

"Base de dados: O espaço em disco" trabalho analisar o crescimento do banco de dados e faz a estimativa se haverá espaço suficiente para a próxima operação como backup (incluindo teste de restauração) no disco rígido específico.

Ele gera vários tipos de alertas. Problemas com espaço em disco estão no topo da lista de motivos de corrupção, por isso preste atenção aos alertas após o início do job.

Este trabalho também contribui com dados para o gráfico de análise de espaço no servidor.

Por padrão, esse trabalho está habilitado.

Usando o diálogo de configuração, você pode especificar a verificação dos períodos e dos limites para o espaço livre. O primeiro limiar alcançado será alertado. Para definir o limite só em% do espaço em disco, você precisa definir o espaço explícita em bytes para "-1".

4.19. Database: Database statistics

Este job é muito útil para capturar problemas de desempenho e realizar uma checagem geral do banco de dados de baixo nível, sem fazer backup.

Recomendamos executar esse trabalho todos os dias e guardar um histórico de relatório de estatísticas.

Usando o IBAnalyst (<http://www.ibanalyst.com>) é possível descobrir problemas profundos com o desempenho do banco de dados.

Como um efeito colateral útil, estatísticas visitar todas as páginas do banco de dados para tabelas e índices, e assegura que todos eles estão corretos.

Database statistics configuration

Enabled

Schedule: 0 0 21 ? * MON-FRI

Store stats in: \${db.default-directory}/\${job.id}

Stats archive depth: 7

Stats file name pattern: {0,date,yyyyMMdd_hh_mm}.stats

Save Cancel

4.20. Database: Send logs

“Database: Send logs” é um job auxiliar que envia os logs de postos de trabalho de nível de banco de dados por e-mail com a frequência desejada.

Este trabalho é desativado por padrão.

Se o banco de dados monitorado está situado em local remoto é útil para agendar o envio de registros por e-mail. Usando o diálogo de configuração, você pode agendar o envio de registros com uma expressão do CRON (para mais detalhes veja [Apêndice: expressões do CRON](#)), especificar a partir de que e-mail que será enviado e para onde. Definição das configurações de alertas de e-mail ser utilizada (para mais detalhes veja [3.5. Alerta de email no FBDataGuard](#)).

Send database logs

Enabled

Schedule: 0 0 23 ? * MON-FRI

E-mail from: dataguard@here.com

E-mail to: whoami@whereami.com

Jobs ids: disk-space, backup, collect-stats, active-users, validate-db

Save Cancel

Além disso, você pode especificar os logs dos trabalhos que você precisa para enviar especificando o Jobs IDs.

5. FBDataGuard dicas e truques

FBDataGuard permite mudar sua configuração, não só através de web-console, mas também através de modificação direta de arquivos de configuração. Isto pode ser útil quando você precisa instalar FBDataGuard no modo silencioso (sem interação com o usuário), para empacotá-lo com software de terceiros, ou para realizar alguns ajustes de configurações finas.

5.1. Path para configuração FBDataGuard

O iniciar FBDataGuard procura pelo arquivo **DataGuardJavaSvc.ini** – e ele pode ser localizado próximo ao executável **DataguardJavaSvc.exe**. No final desse arquivo você verá:

param04 =-config-directory=G:\temp2\FBDataGuard\config

param05 =-default-output-directory=G:\temp2\FBDataGuard\output

Se você deseja agrupar o FBDataGuard com software de terceiros, e construir a configuração manualmente, você precisa escrever os caminhos adequados nesta ini (veja)

5.2. Adjusting web-console port

Uma das perguntas mais freqüentes é como ajustar a porta para a aplicação web-console (por padrão é 8082), ele pode ser feito alterando a configuração da porta no arquivo

%config%\agent\agent.properties

server.port = 8082 #change it

%config% -Pasta para armazenar as configurações. Veja em [FBDataGuard permite mudar sua configuração](#), não só através de web-console, mas também através de modificação direta de arquivos de configuração. Isto pode ser útil quando você precisa instalar FBDataGuard no modo silencioso (sem interação com o usuário), para empacotá-lo com software de terceiros, ou para realizar alguns ajustes de configurações finas.

5.1. Path para configuração FBDataGuard

Apêndice: expressões do CRON

Todos os trabalhos em FBDataGuard têm configurações de tempo em formato cron. CRON é um formato muito fácil e poderoso para programar tempos de execução.

Formato CRON

Uma expressão do CRON é uma string a string composta de 6 ou 7 campos separados por espaços em branco. Os campos podem contar qualquer dos valores habilitados, juntamente com várias combinações de caracteres especiais permitidos para aquele campo. Os campos são como se segue:

Nome do campo	Obrigatório	Valores permitidos	Caracteres especiais permitidos
Seconds	SIM	0-59	, - * /
Minutes	SIM	0-59	, - * /
Hours	SIM	0-23	, - * /
Day of month	SIM	1-31	, - * ? / L W
Month	SIM	1-12 or JAN-DEC	, - * /
Day of week	SIM	1-7 or SUN-SAT	, - * ? / L #
Year	NÃO	empty, 1970-2099	, - * /

Então as expressões do cron são bem simples como: * * * * ? *


ou mais complexas como essa: 0 0/5 14,18,3-39,52 ? JAN,MAR,SEP MON-FRI 2002-2010

Caracteres especiais


- * ("*todos valores*") - usado para selecionar todos os valores dentro de um campo. Por exemplo, "*" no campo minuto significa "a cada minuto".
- ? ("nenhum valor específico") - útil quando você precisa especificar algo em um dos dois campos em que o personagem é permitido, mas não o outro. Por exemplo, se eu quero que minha trigger dispare em um determinado dia do mês (por exemplo, o 10^o), mas não me importo com os dias da semana que sejam, eu colocaria "10" no dia do mês (day-of-month), e "?" no campo de dia da semana (day-of-week). Veja os exemplos abaixo para esclarecimentos.
- - -usado para especificar faixas. Por exemplo, "10-12" no campo hora significa "*nas horas 10, 11 e 12*".
- , - usado para especificar valores adicionais. Por exemplo, "MON,WED,FRI" no campo dia da semana (day-of-week) significa "*Nos dias Segunda (Monday), Quarta (Wednesday) e Sexta (Friday)*".
- / - usado para especificar incrementos. Por exemplo "0/15" no campo segundos significa "*nos segundos 0, 15, 30, e 45*". E "5/15" no campo segundos significa "*nos segundos 5, 20, 35 e 50*". Você também pode especificar '/' depois do "**character - in this case** " que é equivalente a ter um '0'

antes da '/'. '1/3' no campo dia do mês (day-of-month) "*dispara a cada 3 dias iniciando no primeiro dia do mês*".

- **L** ("*last*") - tem um significado diferente em cada um dos dois campos em que é permitida. Por exemplo, o valor "L" no campo o dia do mês significa "o último dia do mês" - dia 31 de janeiro, dia 28 de fevereiro em anos não-bissextos. Se usado no campo de dia da semana, por si só, significa simplesmente "7" ou "SAT". Mas, se usado no campo de dia da semana após outro valor, isso significa que "o último dia do mês xxx" - por exemplo, "6L" significa "a última sexta-feira do mês". Ao usar a opção 'L', é importante não especificar listas, ou intervalos de valores, pois poderá obter resultados confusos.
- **w** ("*weekday*") – usado para especificar o dia da semana (dia útil: segunda a sexta-feira) mais próxima do dia determinado. Como exemplo, se você especificar "15W" como o valor para o campo do dia do mês, o significado é: "o dia da semana útil mais próximo ao dia 15 do mês." Assim, se o 15 é um sábado, o gatilho será acionado na sexta-feira dia 14. Se o dia 15 é um domingo, o gatilho será acionado na segunda-feira dia 16. Se o dia 15 é uma terça-feira, então ele vai disparar na terça-feira dia 15. No entanto, se você especificar "1W" como o valor para o dia do mês, e o primeiro é um sábado, o gatilho será acionado na segunda-feira dia 3, já que não vai "saltar" sobre o limite de dias de um mês. O caractere 'W' só pode ser especificado quando o dia do mês é um único dia, não um intervalo ou lista de dias.

 Os caracteres 'L' e 'W' também podem ser combinados no campo dia do mês (day-of-month) que significará "*última semana do mês*".

- **#** - usado para especificar "o enésimo" XXX dia. Por exemplo, o valor de "6#3" no campo de dia da semana significa "terceira sexta-feira do mês" (dia 6 = sexta e "#3" = a terceira no mês). Outros exemplos: "2#1" = a primeira segunda-feira do mês e "4#5" = a quinta quarta-feira do mês. Note que se você especificar "#5" e não há cinco de um determinado dia da semana, no mês, então nenhum disparo ocorrerá esse mês.

 Os caracteres e os nomes dos meses e dias da semana não são case sensitive. MON é o mesmo que mon.

Exemplos do CRON

Alguns exemplos completos:

Expressão	Significado
0 0 12 * * ?	Dispara as 12:00 (meio-dia) todo dia
0 15 10 ? * *	Dispara as 10:15 todo dia
0 15 10 * * ?	Dispara as 10:15 todo dia
0 15 10 * * ? *	Dispara as 10:15 todo dia
0 15 10 * * ? 2005	Dispara as 10:15 todo dia durante o ano de 2005

0 * 14 * * ?	Dispara a todo minuto iniciando as 14:00 e terminando as 14:59, todo dia
0 0/5 14 * * ?	Dispara a cada cinco minutos a partir de 14:00 e terminando às 02:55, todos os dias
0 0/5 14,18 * * ?	Dispara a cada cinco minutos a partir de 14:00 e terminando às 02:55, e também dispara a cada 5 minutos a partir de 06:00 e terminando às 06:55, todos os dias
0 0-5 14 * * ?	Dispara a cada minuto a partir das 14:00 e terminando às 14:05, todos os dias
0 10,44 14 ? 3 WED	Dispara as 14:10 e as 02:44 toda quarta-feira no mês de março.
0 15 10 ? * MON-FRI	Dispara às 10:15 toda segunda-feira, terça, quarta, quinta e sexta-feira
0 15 10 15 * ?	Dispara às 10:15 no dia 15 de cada mês
0 15 10 L * ?	Dispara às 10:15 no último dia de cada mês
0 15 10 ? * 6L	Dispara às 10:15 na última sexta-feira de cada mês
0 15 10 ? * 6L	Dispara às 10:15 na última sexta-feira de cada mês
0 15 10 ? * 6L 2002-2005	Dispara às 10:15 em cada última sexta-feira de cada mês, durante os anos de 2002, 2003, 2004 e 2005
0 15 10 ? * 6#3	Dispara às 10:15 na terceira sexta-feira de cada mês
0 0 12 1/5 * ?	Dispara às 12h (meio-dia) a cada 5 dias a cada mês, começando no primeiro dia do mês.
0 11 11 11 11 ?	Dispara todo 11 de novembro às 11:11 horas.



Preste atenção no uso de '?' e '*' nos campos day-of-week (dia da semana) e day-of-month (dia do mês)!

Notes

- Suporte para especificar tanto o dia da semana como um dia do mês simultaneamente não está complete (você deve usar atualmente o caractere '?' em um desses campos).
- Tenha cuidado quando configurar hora de disparo (fire times) entre a meia noite e uma hora da manhã - "horário de verão" pode causar um salto ou a repetição da ação dependendo da forma que o tempo se altera (adianta ou atrasa).

Mais informação aqui:

<http://www.quartz-scheduler.org/docs/tutorials/crontrigger.html>

6. Contato do suporte

Nós vamos responder a todas suas perguntas sobre FBDataGuard. Por favor envie perguntas para support@ib-aid.com