

Conceitos de Banco de Dados

Aula 10 - Backup On-Line e Off-Line

Apresentação

Olá! Nas aulas anteriores você estudou a linguagem SQL, como criar tabelas, inserir, atualizar e remover dados. Além disso, aprendeu como alterar a estrutura das tabelas, adicionando, removendo ou modificando suas colunas. Viu também como escrever consultas simples e consultas avançadas com múltiplas tabelas e ainda criou subconsultas, visões (*views*), procedimentos armazenados (*stored procedures*) e funções.

Nesta aula, você conhecerá a importância dos backups e seus tipos existentes, fará o procedimento necessário para realizar uma cópia de segurança (DUMP) de uma base de dados, e aprenderá como restaurá-la em uma nova base de dados.

Objetivos

- Conhecer a importância da realização de *backups*
- Diferenciar *backup* off-line do *backup* on-line
- Entender e realizar DUMP de uma base de dados no MySQL Server
- Entender e restaurar DUMP em uma base de dados no MySQL Server

O que são Backups?

Acredito que você já deve ter ouvido falar em *backup*, é um termo muito conhecido na área de Tecnologia da Informação (TI). É uma expressão do inglês e significa “Cópia de Segurança”.

A realização de cópias de segurança, em TI, objetiva evitar a perda dos dados das aplicações e, conseqüentemente, dados dos usuários. Já pensou se de uma hora para outra você não conseguisse mais ter acesso ao seu computador? E se, de forma inesperada, o disco de armazenamento de seu computador apresentasse defeito, tornando-o inoperante? Quais dados armazenados nele você provavelmente perderia? Documentos de texto, músicas, vídeos, fotografias que você capturou no último final de semana, ou tantos outros documentos? Quão importante são esses dados para você? Não é fácil prever quando computadores podem apresentar defeito e assim ocorrer a perda de informações armazenadas.

Já imaginou se o ambiente virtual Moodle que você utiliza em nosso curso fosse contaminado por um vírus de computador, o qual apagasse as contas de todos os alunos, mediadores e professores? O que seria do curso a partir desse momento? Todas as postagens dos fóruns, as notas de participação virtual, as notas das atividades que você e seus colegas responderam desde o início do curso, se todos esses dados estivessem perdidos e sem cópia de segurança?

É inimaginável a situação em que se perde parcialmente ou totalmente os dados de uma empresa ou instituição. Essa situação pode ser catastrófica e levar grandes empresas à falência.

Pensando sempre no pior, é importante a realização de backups frequentemente, para diminuir as chances da perda de dados dos usuários e assim diminuir os danos que poderão ser causados caso ocorra uma perda de dados, seja momentânea ou não. Portanto, faça sempre cópias de segurança dos seus dados pessoais para que imprevistos não acarretem em dores de cabeça.

A Importância do Backup

No início da aula, falamos sobre backups e questionamos sobre o que aconteceria se o Moodle utilizado no Instituto Metrópole Digital fosse completamente perdido. Consegue imaginar a frequência com que a perda de dados ocorre? Você acredita que quase nunca há perda de dados na T.I., certo? Não é bem assim, a perda de dados pode parecer algo distante, mas é bem mais frequente do que pensa!

Curiosidade!

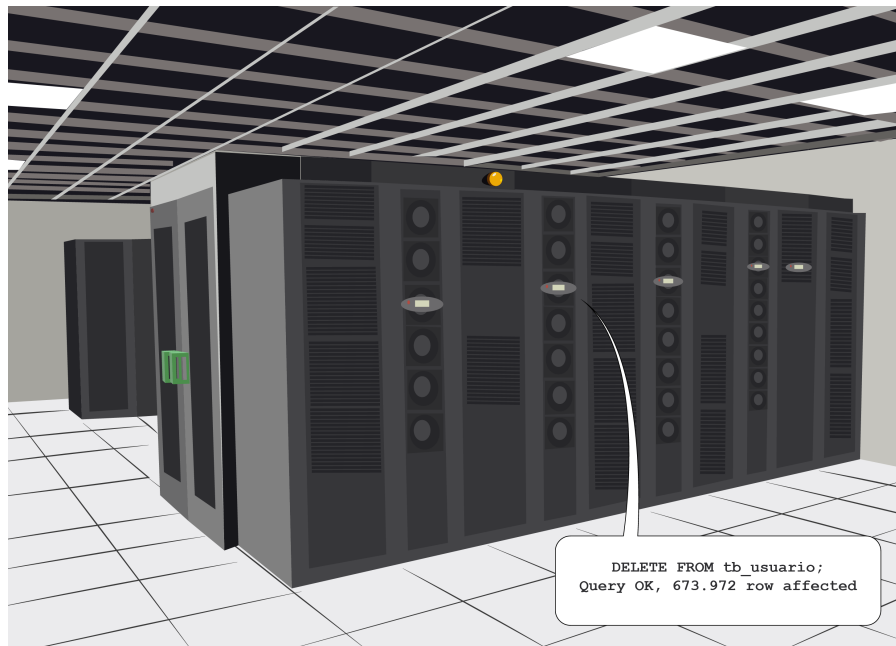
De acordo com a revista Exame, 77% das empresas perderam dados em 2010, implicando no prejuízo de milhões de dólares.

Fonte: Revista Exame. Disponível em: <http://exame.abril.com.br/tecnologia/77-das-empresas-perderam-dados-em-2010-diz-estudo/>. Último acesso em 26 de mar 2017.

Recentemente, o Canaltech no Brasil divulgou uma consulta realizada em 125 organizações, constatando que as empresas enfrentaram prejuízos superiores a US\$ 26 bilhões de dólares (cerca de R\$ 66 bilhões de reais) devido à perda de dados, sendo que mundialmente o montante significou US\$ 1,7 trilhão de dólares (R\$ 4,3 trilhões de reais).

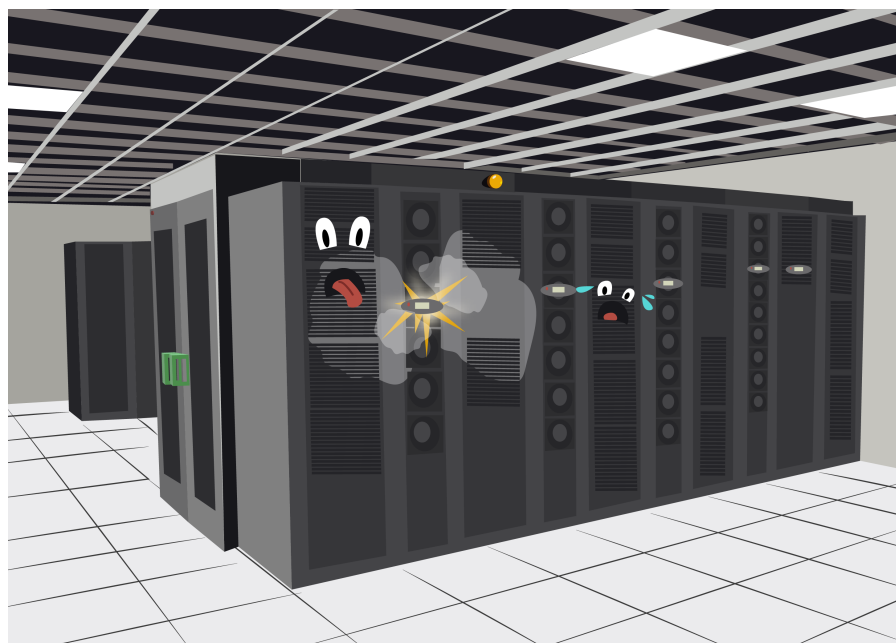
Se há tantos danos, você deve estar se perguntando quais são os principais motivos que podem provocar a perda de dados, certo? Ela pode ser provocada por diversas situações, mas vamos listar algumas e comentá-las rapidamente:

1. **Erro de Software:** uma falha na implementação do software pode provocar a deleção de informações e, conseqüentemente, a perda de dados;



Fonte: Autoria própria.

2. **Superaquecimento:** servidores que não estão com refrigeração adequada podem apresentar falhas ao sobreaquecerem e, em alguns casos, possuir sistemas de segurança que realizam o desligamento automático do equipamento abruptamente para evitar danos físicos ao hardware, essa forma de desligamento poderá corromper sistemas de arquivos;



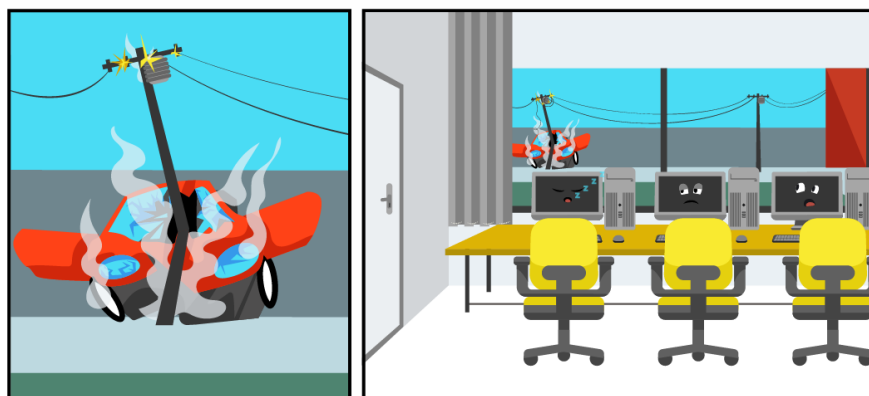
Fonte: Autoria própria.

3. **Umidade e Maresia:** equipamentos expostos à ação da umidade e da maresia, normalmente, possuem um encurtamento de sua vida útil, pois

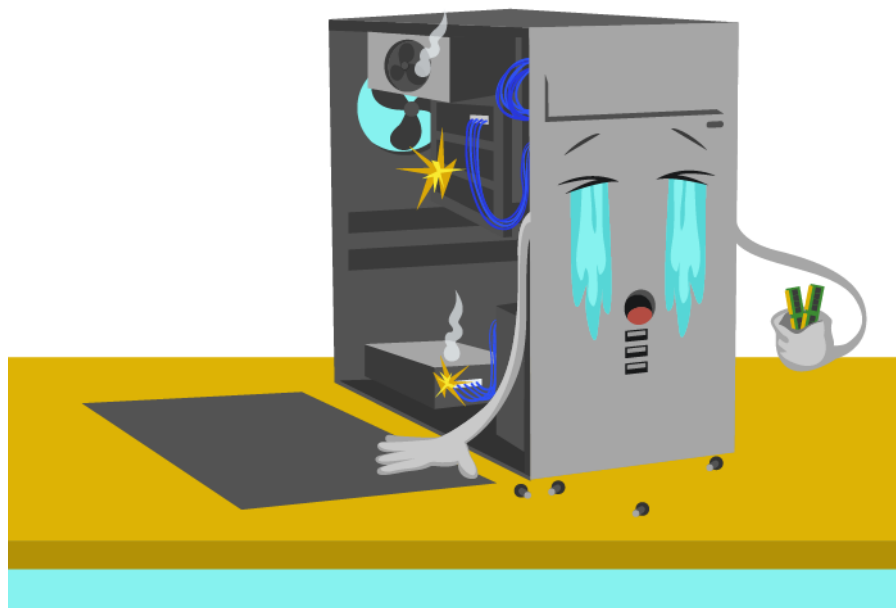
as trilhas e os terminais dos componentes internos do equipamento sofrem oxidação;



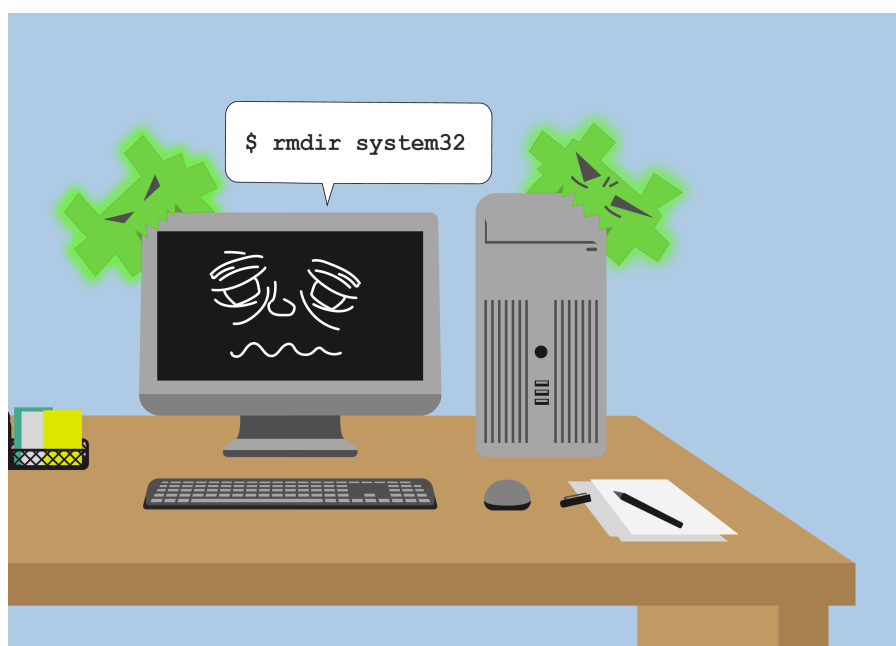
4. **Instabilidade na rede elétrica e quedas de energia:** o fornecimento de energia elétrica para um computador é primordial e se, por algum motivo, houver falhas inesperadas no fornecimento, o desligamento abrupto do equipamento poderá corromper tabelas de bancos de dados ou até mesmo o sistema de arquivos do sistema operacional;



5. **Máquinas descartáveis (baixa qualidade do hardware):** muitas vezes, buscando economizar dinheiro, algumas instituições utilizam computadores com componentes eletrônicos de baixa qualidade e que não foram construídos para funcionarem 24h por dia/7 dias por semana. Por esse motivo, esses equipamentos podem apresentar falhas inesperadas quando em operação e com sobrecarga de processamento.



6. **Vírus:** os vírus atuais estão cada vez mais complexos, alguns deles criptografam os arquivos do servidor, inviabilizando a leitura destes e o acesso à senha necessária para descriptografar. Outros vírus podem realizar comandos no computador, apagando os dados nele existentes;

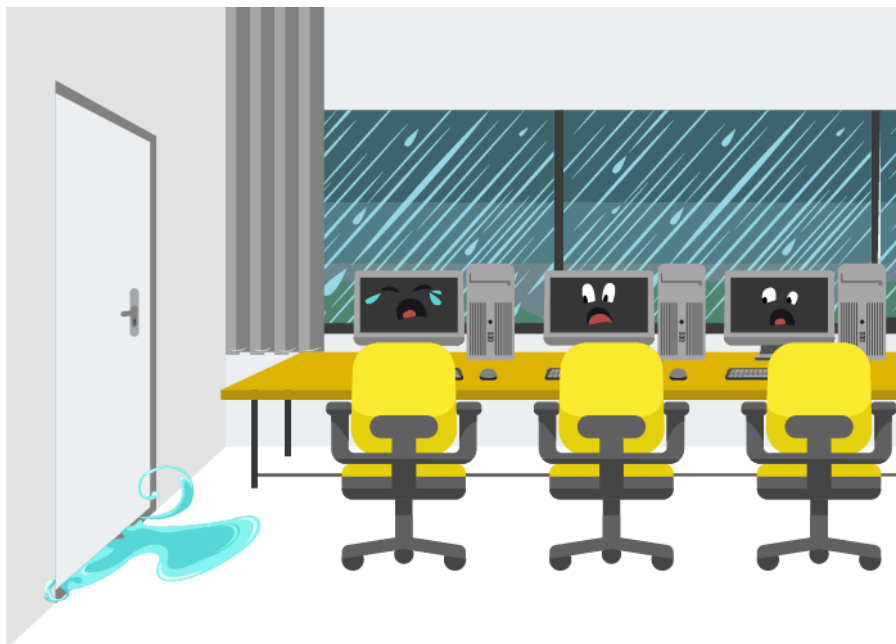


Fonte: Autoria própria.

7. **Código Hacking/Cracking:** Um cracker poderá obter acesso indevido aos servidores e nele realizar operações que provoquem a perda de dados, seja apagando os arquivos ou mesmo criptografando-os;



8. **Desastres naturais:** Desastres naturais, como inundações ou terremotos, podem provocar danos físicos aos equipamentos;

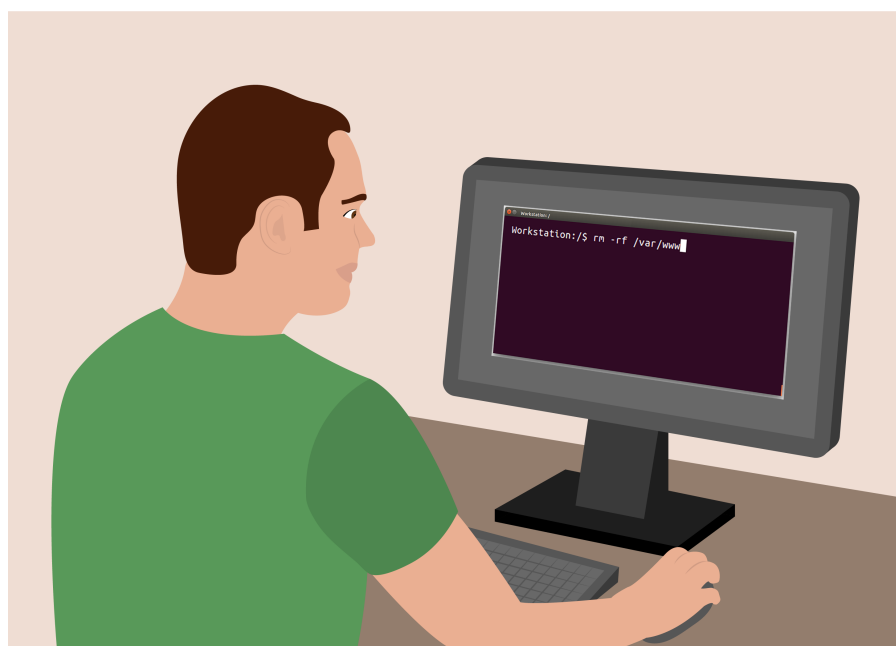


9. **Incêndio:** Uma sobrecarga na rede elétrica poderá provocar um curto e possivelmente iniciar um incêndio no ambiente, e caso atinja a sala onde estão armazenados os servidores, o fogo poderá destruir todos os equipamentos;



Fonte: Autoria própria.

10. **Erro humano:** Um usuário com permissões de administrador poderá realizar acidentalmente ações nos computadores de forma que provoque a perda de dados e arquivos.



Fonte: Autoria própria.

Após listarmos algumas das causas que podem provocar a perda de dados e arquivos, veremos agora os tipos de *backups* e caracterizá-los, conhecendo algumas das vantagens e desvantagens dessas estratégias.

Antes disso, faremos uma breve atividade a seguir.

Atividade 01

1. Pesquise na internet sobre desastres em Data Centers pelo mundo e os danos que foram provocados por esses acontecimentos. Faça uma lista dos principais motivos que causaram esses desastres e, ao final, comente o resultado de sua pesquisa em nosso fórum.

Backup Off-line

O termo “*backup off-line*” é uma referência ao modo como os dados do backup são armazenados. Quando utilizamos essa estratégia, os dados são, geralmente, salvos em mídias físicas.

Estes são alguns exemplos de mídias físicas:

- CDs
- DVDs
- Blu-ray
- Fita magnética
- HDs externo
- Pendrive
- Cartão de Memória



Vamos conhecer agora as inúmeras **vantagens** na utilização dessas mídias:

- **Velocidade:** realizar a gravação dos dados referente à cópia de segurança será, provavelmente, rápida, e geralmente limita-se à capacidade de gravação do dispositivo ou mídia de armazenamento escolhida. O mesmo vale para o momento em que for necessário realizar a restauração dos dados. Imagine que você precise armazenar 180GB de dados, quanto tempo será necessário para copiar essas informações para um HD externo com velocidade de gravação de aproximadamente 20Mega Bytes/s? Cerca de 2 horas e 30 minutos.
- **Fácil acesso:** é comum, ao realizar o backup em mídias físicas e dispositivos de armazenamento, estes serem guardados próximo ao local onde foi gerado o backup. Assim, é possível ter em mãos, rapidamente, as mídias de armazenamento para que possamos realizar o processo de restauração.
- **Transporte:** O transporte de DVDs, Blu-rays, HD Externos, cartões de memória, etc. é leve e fácil de transportar e, desse modo, é possível levar os backups para outro local quando necessário.
- **Segurança:** Pelas cópias estarem armazenadas de forma “off-line”, ou seja, não podem ser acessadas pela Internet, um vírus ou um

cracker que realize um ataque no servidor não conseguirá afetar as cópias de segurança.

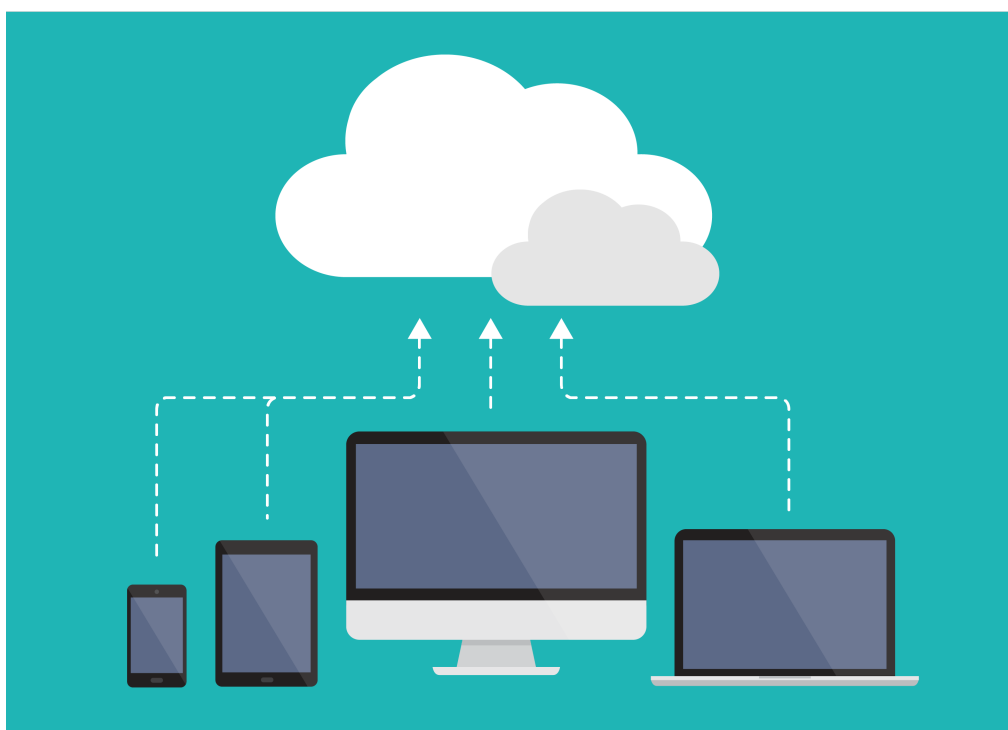
Há também **desvantagens** na utilização da estratégia de backup off-line, conheça algumas:

- **Facilmente destruído:** Como vimos no início da nossa aula, há ocasiões em que podem ocorrer danos físicos nos locais onde ficam armazenados os servidores. Isso também afeta as mídias de armazenamento como CDs e DVDs, a camada responsável pela reflexividade do disco possui elementos metálicos e eles podem oxidar, fazendo com que o disco não possa ser lido pelo equipamento. Além disso, um incêndio poderia destruir todas as mídias de armazenamento, como Fitas magnéticas e os HDs Externos.
- **Roubo/Furto:** Outro risco que também pode afetar os backups off-line refere-se aos furtos. O local onde estão armazenados os backups poderá ter seus itens subtraídos e consequentemente os dados serão levados. Outro detalhe é que se os dados presentes nas mídias não estiverem criptografados poderão ser acessados pelo assaltante e se houver dados sensíveis (como números de documentos, números de cartões de crédito, senhas de usuários, etc.), poderão ser utilizados em fraudes.
- **Risco de falha tecnológica:** Você já deve ter percebido como as tecnologias evoluem rapidamente, isso também pode ser um problema, caso grave os dados em uma mídia de armazenamento e no momento em que necessitar ler os dados dessa mídia os equipamentos necessários para a leitura dela já não estejam mais funcionando, não sendo possível a compra de um novo equipamento.
- **Limitação de armazenamento:** Se a quantidade de arquivos/dados for superior à capacidade do dispositivo de armazenamento, será necessário dividir o conteúdo em partes. Dependendo da quantidade de partes necessárias para dividir os dados, poderá implicar no aumento de trabalho para organizar essas cópias de segurança. Além disso, a perda de uma dessas partes, dependendo da estratégia de divisão, poderá ocasionar o dano completo da cópia de segurança.

Tudo bem até aqui? Conheceremos agora o chamado “backup on-line” e as suas características, assim como as vantagens e as desvantagens desses recursos. Vamos lá?

Backup On-line

Na estratégia do backup on-line os dados são salvos “na Internet”, ou seja, não utilizamos o armazenamento de forma física local. Os serviços de backup on-line estão cada vez mais populares e essa opção tem se difundido rapidamente na atualidade.



Assim como os backups off-line, a estratégia de realizar backups on-line também possui vantagens e desvantagens, vamos conhecer primeiro algumas das **vantagens**:

- **Acessível em qualquer lugar:** os backups estão acessíveis em qualquer lugar do mundo com acesso à Internet, não importa se você está conectado pela rede de dados 3G/4G de seu aparelho celular ou através de um acesso por fibra óptica de alta velocidade.

- **Roubo/Furto:** caso alguma ocorrência de roubo ocorra e os equipamentos da instituição sejam furtados, os backups estarão protegidos por estarem inacessíveis fisicamente, tal qual os equipamentos presentes no local.
- **Proteção contra danos naturais:** devido os backups não estarem fisicamente no mesmo ambiente dos dados de origem, caso ocorra alguma catástrofe natural que destrua os equipamentos da instituição, como inundações ou mesmo incêndios, as cópias de segurança estão protegidas em outro local, possivelmente até em outro continente.
- **Segurança da criptografia:** geralmente, ao enviar os backups através da Internet para um servidor localizado fisicamente em outro local, os softwares responsáveis pela automatização desse processo primeiramente realizam a criptografia dos dados para, então, enviá-los através da Internet.

Podemos dizer que as **desvantagens** dos backups on-line estão diretamente relacionadas às suas vantagens. Vejamos:

- **Localização física dos dados:** ao utilizarmos essa estratégia de backup on-line, torna-se difícil saber exatamente em qual lugar ou máquina os dados foram salvos.
- **Dependência da conexão com a Internet:** toda ação ao realizar um backup ou restauração depende diretamente da conexão com a Internet. Se, por qualquer motivo, a conexão for interrompida por muito tempo (como dias ou semanas) os backups poderão ser interrompidos ou ficarem defasados.
- **Velocidade de conexão:** a velocidade de conexão com a Internet irá interferir no tempo necessário para enviar os backups pela Internet. Tanto a velocidade de upload como a de download impactam diretamente no envio e no recebimento dos arquivos. Se a frequência de realização dos backups for alta e o tamanho dos arquivos for elevado, o tempo necessário para copiar todos os arquivos poderá ser inviável.

Saiba Mais!

Considere que você necessita armazenar os backups do Moodle do IMD e estes estão com mais de 100GB de dados. Com base no que você estudou até agora, avalie as melhores mídias físicas e alguns serviços de backup on-line.

Sugestão: Pesquise sobre armazenamento em fitas magnéticas (mídias físicas) e sobre os serviços Dropbox, Google Drive, OneDrive e AWS. Monte uma tabela das capacidades de armazenamento e do custo para se utilizar essas soluções. Você pode compartilhar nos fóruns ou no encontro presencial o resultado de sua pesquisa e compará-lo com os de seus colegas!

Utilizando o mysqldump

Agora que você já sabe o que são backups, que tal realizarmos cópias de segurança dos bancos de dados criados durante nossa disciplina? Para isso, vamos utilizar um programa que é fornecido com o MySQL Server e que se chama mysqldump.

O mysqldump é um utilitário que executa uma série de comandos para gerar cópias integrais ou parciais de um banco de dados. Através dele é possível gerar arquivos com conjuntos de instruções SQL, as quais poderão ser executadas para recriar o banco de dados do qual realizamos a cópia de segurança e, assim, será possível recriar as tabelas que existiam no banco de dados original.

Além de recriar a estrutura das tabelas, o arquivo gerado pelo mysqldump também possui os comandos para inserir os mesmos dados que estavam presentes nas tabelas do banco, refletindo o momento em que o backup foi gerado.

O arquivo gerado pelo mysqldump recebe o nome de **dump**. Então, vamos criar agora o nosso **dump** da base de dados **locadora** que desenvolvemos durante a nossa disciplina?

O primeiro passo é a abertura de uma janela de terminal, lembra-se da aula de Segurança em que não utilizamos o MySQL Command Client e sim o *prompt* do sistema operacional? Esse prompt será necessário para criarmos a cópia do banco **locadora** com o mysqldump.

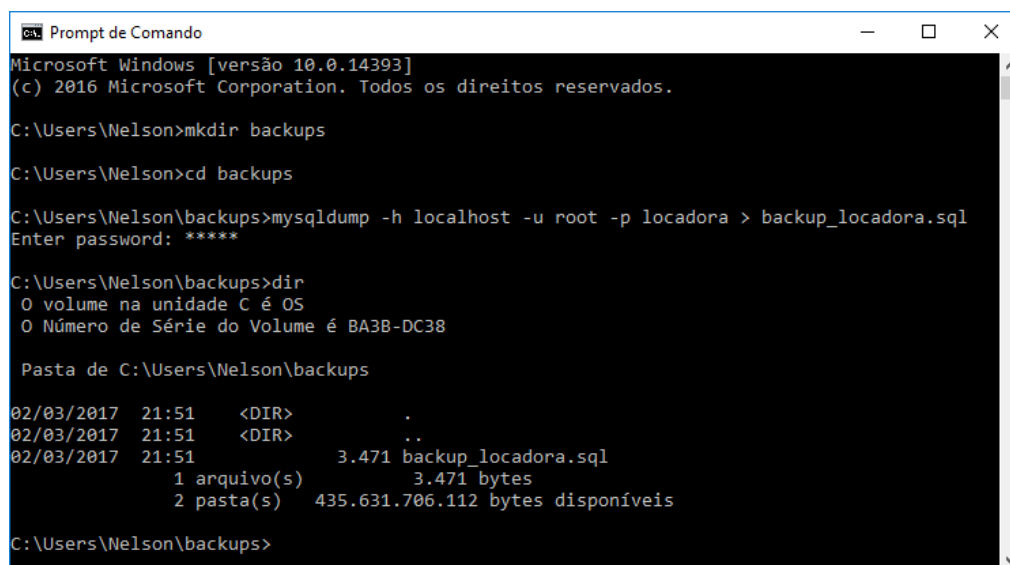
Na **Figura 1**, criamos um diretório chamado **backups**, utilizando o comando **mkdir**, em seguida acessamos o diretório com o comando **cd**. Após o acesso ao diretório backups, utilizamos o comando cuja sintaxe é:

```
1 mysqldump -h endereço_do_servidor -u usuário -p banco_de_dados > nome_do_arquivo_que_será
```

Observe na **Figura 1** que o comando digitado foi:

```
1 mysqldump -h localhost -u root -p locadora > backup_locadora.sql
```

Figura 01 - Prompt do DOS com o comando mysqldump para o banco de dados locadora.



```
Prompt de Comando
Microsoft Windows [versão 10.0.14393]
(c) 2016 Microsoft Corporation. Todos os direitos reservados.

C:\Users\Nelson>mkdir backups

C:\Users\Nelson>cd backups

C:\Users\Nelson\backups>mysqldump -h localhost -u root -p locadora > backup_locadora.sql
Enter password: *****

C:\Users\Nelson\backups>dir
O volume na unidade C é OS
O Número de Série do Volume é BA3B-DC38

Pasta de C:\Users\Nelson\backups
02/03/2017  21:51    <DIR>          .
02/03/2017  21:51    <DIR>          ..
02/03/2017  21:51                3.471 backup_locadora.sql
               1 arquivo(s)                3.471 bytes
               2 pasta(s)          435.631.706.112 bytes disponíveis

C:\Users\Nelson\backups>
```

Fonte: Captura de tela do mysqldump pelo Autor (2017).

Após pressionarmos a tecla “*enter*” é solicitada a senha, ao final digitamos o comando “**dir**” para verificarmos se o arquivo *backup_locadora.sql* foi criado no diretório atual.

Vamos agora detalhar cada parâmetro do comando que acabamos de executar:

- **mysqldump:** Utilitário que permite realizar a cópia de segurança de um determinado banco de dados;
- **-h:** Parâmetro utilizado para indicar o endereço do servidor no qual o mysqldump deverá conectar-se para poder extrair a cópia do banco de dados;
- **localhost:** O endereço do servidor no qual estamos nos conectando. Nem sempre desejamos executar a cópia de um banco de dados que está sendo executado na máquina local, portanto esse valor poderia ser o endereço de um servidor na internet, como www.imd.ufrn.br;
- **-u:** Parâmetro para indicar que informaremos o nome do usuário utilizado para conectar-se ao banco de dados. O usuário informado deverá ter permissão para executar a cópia do banco de dados;
- **root:** O usuário que estamos informando em nosso comando é o que possui permissão total, no entanto, caso o "josemar" que vimos em aulas anteriores também possua a permissão necessária, ele também poderia realizar um backup do banco de dados locadora;
- **-p:** Indica que ao pressionarmos "enter" o mysqldump deverá solicitar a senha do usuário o qual estamos informando através do parâmetro -u;
- **locadora:** É o nome do banco de dados que desejamos realizar a cópia de segurança;
- **>:** A seta para a direita indica que vamos realizar a cópia do banco de dados em um arquivo;
- **backup_locadora.sql:** É o nome do arquivo o qual será salvo no diretório atual. Lembre-se que estamos dentro do diretório backups criado antes de iniciarmos esse comando.

Visto isso, aprenderemos agora a restaurar um dump no MySQL Server, fique atento a essas orientações e compartilhe em nosso fórum as dúvidas com seus colegas no encontro presencial.

Restaurando um DUMP no MySQL Server

Já sabemos realizar cópias de segurança para cada banco de dado presente em nosso servidor MySQL Server, mas você deve estar pensando:

Tenho a cópia de todos os meus bancos de dados, mas se o banco de dados da minha locadora for apagado por um vírus, como eu posso restaurar a cópia que realizei?

Vamos agora restaurar o banco de dados **locadora**, mas em vez de colocar no mesmo banco de dados, criaremos um novo banco denominado **locadora_teste** para podermos realizar a restauração da cópia que criamos. Nesse momento, você precisará acessar o MySQL Server Command Line e criar o novo banco de dados com o comando:

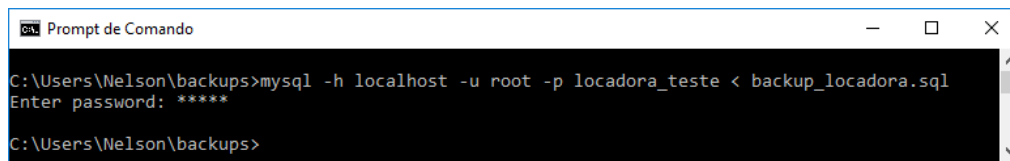
```
1 CREATE DATABASE locadora_teste;
```

Com o novo banco de dados criado, vamos utilizar, no prompt do sistema operacional, o comando `mysql` para restaurar o dump que criamos anteriormente. A sintaxe do comando é bem semelhante ao de criar a cópia de segurança, veja o comando abaixo:

```
1 mysql -h endereço_do_servidor -u usuário -p nome_do_banco_de_dados < arquivo_dump
```

Observe a **Figura 2** e note o comando completo que utilizamos para restaurar o dump criado do banco de dados **locadora** no novo banco chamado **locadora_teste**.

Figura 02 - Prompt do DOS com o comando mysql para restaurar um dump do banco de dados locadora no banco de dados locadora_teste.



```
Prompt de Comando

C:\Users\Nelson\backups>mysql -h localhost -u root -p locadora_teste < backup_locadora.sql
Enter password: *****
C:\Users\Nelson\backups>
```

Fonte: Captura de tela do mysqldump pelo Autor (2017).

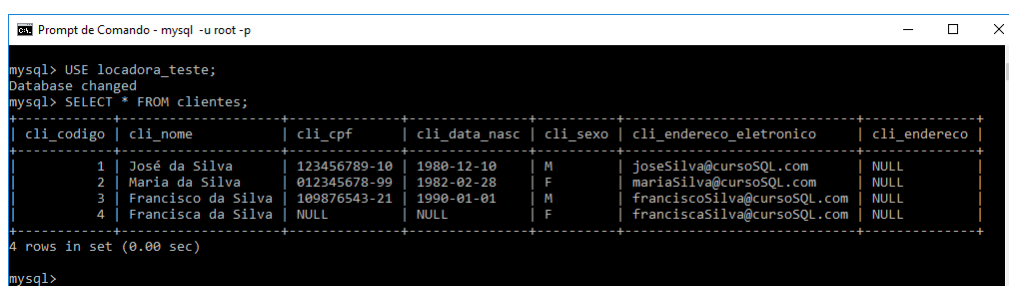
Veja agora, detalhadamente, cada parâmetro do comando que acabamos de executar:

- **mysql:** Utilitário que permite realizar, dentre outras ações, a restauração de uma cópia de segurança para um banco de dados;
- **-h:** Parâmetro utilizado para indicar o endereço do servidor no qual o mysql deverá conectar-se para poder restaurar um dump de banco de dados;
- **localhost:** O endereço do servidor no qual estamos nos conectando. Nem sempre desejamos executar a restauração de dump em um banco de dados que está sendo executado na máquina local, portanto esse valor poderia ser o endereço de um servidor na internet, como www.imd.ufrn.br;
- **-u:** Parâmetro para indicar que informaremos o nome do usuário o qual utilizaremos para conectar-se ao banco de dados. O usuário informado deverá ter permissão para criar tabelas e inserir registros no banco de dados;
- **root:** O usuário que estamos informando em nosso comando é o que possui permissão total;
- **-p:** Indica que ao pressionarmos enter o mysql deverá solicitar a senha do usuário que estamos informando através do parâmetro -u;
- **locadora_teste:** é o nome do banco de dados que desejamos, o qual irá receber o dump;

- <: A seta para a esquerda indica que vamos realizar a cópia do arquivo dump no banco de dados;
- **backup_locadora.sql**: É o nome do arquivo dump que geramos com o mysqldump.

Se tudo correu como esperado, devemos agora acessar o nosso banco de dados e verificar se os dados foram restaurados. Veja a e observe que acessamos o banco de dados locadora_teste e então realizamos uma consulta SELECT na tabela clientes:

Figura 03 - Prompt do DOS com os comandos USE locadora_teste e SELECT * FROM clientes.



```
mysql> USE locadora_teste;
Database changed
mysql> SELECT * FROM clientes;
```

cli_codigo	cli_nome	cli_cpf	cli_data_nasc	cli_sexo	cli_endereco_eletronico	cli_endereco
1	José da Silva	123456789-10	1980-12-10	M	joseSilva@cursoSQL.com	NULL
2	Maria da Silva	012345678-99	1982-02-28	F	mariaSilva@cursoSQL.com	NULL
3	Francisco da Silva	109876543-21	1990-01-01	M	franciscoSilva@cursoSQL.com	NULL
4	Francisca da Silva	NULL	NULL	F	franciscaSilva@cursoSQL.com	NULL

```
4 rows in set (0.00 sec)

mysql>
```

Fonte: Captura de tela do mysqldump pelo Autor (2017).

Tudo certo? Encerramos por aqui a nossa aula sobre backups, conhecemos a existência dos riscos na perda de dados armazenados. Aprendemos como realizar cópia de segurança de um banco de dados no MySQL Server e ainda vimos quais os comandos necessários para criar e restaurar o dump.

Resumo

Nesta aula, conhecemos a importância das cópias de segurança (backups) e os tipos existentes, aprendemos como realizar cópias de bancos de dados presentes no MySQL Server e, em seguida, como realizar a restauração desse dump em um novo banco de dados.

Essa foi a nossa última aula da disciplina de Conceitos de Banco de Dados, espero que tenham gostado dos conteúdos vistos e que as dúvidas existentes tenham sido respondidas em nossos fóruns. Até a próxima, pessoal!

Autoavaliação

1. Agora que você entendeu como realizar o backup do banco de dados locadora, verifique os bancos de dados que você criou no MySQL Server e realize uma cópia de segurança de todos eles.
2. Tente agora criar uma cópia de segurança de todos os seus bancos de dados com o usuário "Josemar" que você cadastrou nas aulas anteriores.

Referências

Boas Práticas em Backup By Veezor.com. Disponível em: <<https://www.youtube.com/watch?v=BEuuhE8aCwg>>. Acesso em: 25 fev. 2017.

77% das empresas perderam dados em 2010, diz estudo. Disponível em: <<http://exame.abril.com.br/tecnologia/77-das-empresas-perderam-dados-em-2010-diz-estudo/>> Acesso em: 25 fev. 2017.

Empresas brasileiras têm prejuízo de US\$ 26 bi com perda de dados, aponta estudo. Disponível em: <<https://corporate.canaltech.com.br/noticia/protecao-de-dados/Empresas-brasileiras-tem-prejuizo-de-US-26-bi-com-perda-de-dados-aponta-estudo/>>. Acesso em: 26 fev. 2017.

Como o Google perdeu e devolveu milhares de contas do Gmail? Disponível em: <<http://hypescience.com/como-o-google-perdeu-e-devolveu-milhares-de-contas-do-gmail/>>. Acesso em 26 fev. 2017.

Online Backup vs Offline Backup – 2016 Edition. Disponível em: <<https://www.bestbackups.com/online-backup-vs-offline-backup-2016-edition/>>. Acesso em 27 fev. 2017.

MYSQL 5.7 Reference Manual: mysql — The MySQL Command-Line Tool. Disponível em: <<https://dev.mysql.com/doc/refman/5.7/en/mysql.html>>. Acesso em: 02 mar. 2017.

MYSQL 5.7 Reference Manual: mysqldump — A Database Backup Program. Disponível em: <<https://dev.mysql.com/doc/refman/5.7/en/mysqldump.html>>. Acesso em: 02 mar. 2017.