POLÍTICA DE BACKUP

Objetivo

Garantir a integridade e a disponibilidade dos dados do banco de dados do **MusiTon** através de backups periódicos, permitindo a recuperação em caso de falhas, corrupção de dados ou desastres.

Escopo

Esta política abrange o backup do banco de dados do **MusiTon**, armazenado no PostgreSQL, incluindo: backups diários com retenção de 30 dias, backups mensais com retenção de 12 meses e backups anuais mantidos indefinidamente.

Responsabilidades

1. Administrador de Dados:
    - Garantir que os backups sejam realizados nos horários agendados;
    - Verificar periodicamente a integridade dos backups;
    - Configurar e monitorar os scripts de backup.
2. Desenvolvedor de Banco de Dados:
    - Gerenciar backups e recuperação de dados;
    - Criar rotinas automatizadas para execução e monitoramento de backups.
3. Gestor de TI:
    - Coordenar o armazenamento seguro dos backups;
    - Garantir que os backups sejam acessíveis em caso de necessidade de restauração;
    - Supervisionar e atualizar as rotinas de backup conforme necessário.

Diretrizes

1. Horário dos Backups:
    - Todos os backups devem ser realizados às 2h00.
2. Local de Armazenamento:
    - Diretório principal: ***C:\Backups\MusiTon***
    - Subdiretórios:
        - Diários: ***C:\Backups\MusiTon\Diarios***
        - Mensais: ***C:\Backups\MusiTon\Mensais***
        - Anuais: ***C:\Backups\MusiTon\Anuais***
3. Retenção de Dados:
    - Backups Diários:
        - Retidos por 30 dias;
        - Após esse período, backups mais antigos serão excluídos automaticamente.

- Backups Mensais:
    - Retidos por 12 meses;
    - Após esse período, backups mais antigos serão excluídos automaticamente.
- Backups Anuais:
    - Mantidos indefinidamente.

4. Formato de Backup:
    - Os backups serão gerados no formato **custom** do PostgreSQL para facilitar a restauração.

Procedimentos

1. Criação de Diretórios
    - Crie os seguintes diretórios para armazenar os backups:
        - ***C:\Backups\MusiTon\Diarios***
        - ***C:\Backups\MusiTon\Mensais***
        - ***C:\Backups\MusiTon\Anuais***
2. Configuração do Acesso ao Banco de dados
    - Configure o arquivo ***.pgpass*** para armazenar credenciais e evitar solicitações de senha:
        - Localize a pasta ***%APPDATA%***
        - Crie um arquivo ***.pgpass*** com a seguinte estrutura:

          localhost:5432:MusiTon:<usuario>:<senha>

        - Configure as permissões para que apenas o usuário tenha acesso:

          icacls "%APPDATA%\.pgpass" /inheritance:r /grant %USERNAME%:R

3. Criação dos Scripts de Backup
    - Backup Diário:
        - Nome do arquivo: ***backup_diario.bat***
        - Conteúdo:

          @echo off

          set PGPASSWORD=<sua_senha>

          for /f "tokens=1-4 delims=- " %%a in ('date /t') do set dt=%%d-%%b-%%a

          for /f "tokens=1 delims=:" %%a in ('time /t') do set hr=%%a

          set TIMESTAMP=%dt%_%hr%h

pg_dump -U <seu_usuario> -h localhost -F c -b -v -f "C:\Backups\MusiTon\Diarios\MusiTon_%TIMESTAMP%.backup" MusiTon

forfiles /p "C:\Backups\MusiTon\Diarios" /s /m *.backup /d -30 /c "cmd /c del @file"

- Backup Mensal:
  - Nome do arquivo: ***backup_mensal.bat***
  - Conteúdo:

@echo off

set PGPASSWORD=<sua_senha>

for /f "tokens=1-4 delims=- " %%a in ('date /t') do set dt=%%d-%%b-%%a

set TIMESTAMP=%dt%

pg_dump -U <seu_usuario> -h localhost -F c -b -v -f "C:\Backups\MusiTon\Mensais\MusiTon_Mensal_%TIMESTAMP%.backup" MusiTon

forfiles /p "C:\Backups\MusiTon\Mensais" /s /m *.backup /d -365 /c "cmd /c del @file"

- Backup Anual:
  - Nome do arquivo: ***backup_anual.bat***
  - Conteúdo:

@echo off

set PGPASSWORD=<sua_senha>

for /f "tokens=1-4 delims=- " %%a in ('date /t') do set dt=%%d-%%b-%%a

set TIMESTAMP=%dt%

pg_dump -U <seu_usuario> -h localhost -F c -b -v -f "C:\Backups\MusiTon\Anuais\MusiTon_Anual_%TIMESTAMP%.backup" MusiTon

4. Agendamento de Tarefas
   - Software: Utilize o Task Scheduler do Windows.
   - Configure três tarefas separadas:

    - Backup diário (todos os dias às 2h00, executando ***backup_diario.bat***);
    - Backup mensal (dia 1 de cada mês às 2h00, executando ***backup_mensal.bat***);
    - Backup anual (dia 1 de janeiro às 2h00, executando ***backup_anual.bat***).

Verificação e Manutenção

1. Testes Regulares:
    - Execute testes de restauração trimestrais para garantir que os backups sejam utilizáveis.
2. Monitoramento:
    - Verifique logs de execução dos scripts e eventos no Task Scheduler para confirmar a conclusão bem-sucedida.
3. Capacidade de Armazenamento:
    - Monitore o espaço em disco em ***C:\Backups\MusiTon*** para evitar problemas de capacidade.

Restauração de Backups

1. Para restaurar um backup, utilize o comando:

   pg_restore -U <seu_usuario> -h localhost -d MusiTon -v <caminho_do_arquivo_backup>

Regras de Acesso

1. DBA (Administrador de Banco de Dados):

- O DBA terá permissões completas sobre os diretórios de backup, permitindo a leitura, escrita e exclusão dos arquivos.
- O DBA deve ter acesso total ao banco de dados PostgreSQL para realizar a criação e recuperação de backups.
- O DBA será responsável por gerenciar as credenciais no arquivo ***.pgpass*** para a execução dos backups e deverá garantir que as permissões de acesso sejam corretamente configuradas.
- O DBA poderá modificar, se necessário, os scripts de backup e manutenção para otimizar o processo.

Permissões de Acesso:

- **Diretórios de Backup**: Leitura, escrita e exclusão.
- **Banco de Dados**: Acesso total (GRANT ALL).

- **Scripts**: Permissão de leitura e execução.

2. Desenvolvedor de Banco de Dados (Dev de BD):

- O Dev de BD terá acesso apenas aos scripts de backup, com permissões de leitura e execução, mas não poderá excluir ou modificar os backups diretamente.
- O Dev de BD não deve ter acesso direto à pasta de backup nem permissões de escrita ou exclusão.
- O Dev de BD pode ser responsável pela criação de novos scripts ou pela modificação das rotinas de backup, mas as mudanças devem ser revisadas pelo DBA antes de sua implementação.

Permissões de Acesso:

- **Diretórios de Backup**: Leitura.
- **Banco de Dados**: Acesso limitado, podendo realizar consultas e backups sem permissão de restauração ou exclusão de dados.
- **Scripts**: Leitura e execução.

3. Gestor de TI:

- O Gestor de TI terá acesso ao diretório de backups e será responsável por garantir que os backups sejam armazenados de maneira segura.
- O Gestor de TI poderá acessar os arquivos de backup para realizar auditorias ou verificações, mas não poderá restaurar ou modificar os backups diretamente.
- O Gestor de TI não deve ter acesso direto ao banco de dados nem à execução de backups.

Permissões de Acesso:

- **Diretórios de Backup**: Leitura, sem permissões de escrita ou exclusão.
- **Banco de Dados**: Nenhum acesso direto.
- **Scripts**: Leitura.