Hands-on Lab: RBAC

Implementação de Estrutura de Controle de Acesso Baseado em Papéis

Como você segregaria o acesso a um banco de dados crítico entre Vendedor, Gerente e Admin?

Abertura: O que é RBAC e Por que Importa

O QUE É RBAC?

RBAC (Role-Based Access Control) é um modelo de segurança que controla o acesso aos recursos do banco de dados baseado em papéis (Roles). Em vez de gerenciar permissões para cada usuário individualmente, você cria papéis com conjuntos de permissões e atribui usuários a esses papéis.

PRINCÍPIO DO MENOR PRIVILÉGIO (POLP)

Ninguém tem mais acesso do que o estritamente necessário para realizar sua função. Um vendedor não precisa de DELETE. Um gerente não precisa de DROP. Um analista não precisa de INSERT. Cada papel tem apenas o que precisa.

USUÁRIOS VS PAPÉIS

Aspecto	Usuários	Papéis
Quantidade	Centenas	Poucos (5-10)
Gerenciamento	Complexo	Simples
Consistência	Baixa	Alta
Escalabilidade	Difícil	Fácil

BENEFÍCIOS DA SEGREGAÇÃO

- ✓ Administração centralizada e simples
- ✓ Consistência de permissões entre usuários
- ✓ Facilita auditoria e conformidade
- ✓ Escalabilidade: novos usuários rapidamente
- ✓ Reduz risco de erros e acesso não autorizado

Cenário: Northwind Trading Company

Banco de Dados Simulado

A Northwind Trading Company possui um banco de dados relacional com as seguintes tabelas críticas:

- **Produtos:** Informações de estoque e preço
- **Vendas:** Registros de transações (pedidos)
- **Funcionários:** Dados pessoais e salariais

👤 Vendedor

RESPONSABILIDADE
Registrar vendas e consultar preço/estoque

ACESSO REQUERIDO
SELECT em Produtos; INSERT em Vendas

Risco: Médio

👔 Gerente

RESPONSABILIDADE
Consultar tudo para relatórios, corrigir erros e cadastrar produtos

ACESSO REQUERIDO
SELECT *; UPDATE/INSERT em Produtos e Vendas

Risco: Alto

🔐 Admin

RESPONSABILIDADE
Controle total da estrutura do banco

ACESSO REQUERIDO
ALL PRIVILEGES (incluindo DDL)

Risco: Crítico

Etapa 1: Criar Papéis e Usuários

1 Criar Papel Vendedor

Execute o comando para criar o papel vendedor no banco de dados.

```
CREATE ROLE vendedor;
```

2 Criar Papel Gerente

Execute o comando para criar o papel gerente no banco de dados.

```
CREATE ROLE gerente;
```

3 Criar Papel Admin

Execute o comando para criar o papel admin no banco de dados.

```
CREATE ROLE admin;
```

4 Criar Usuários (João, Maria, Pedro)

Execute os comandos para criar 3 usuários com senhas. Cada usuário será atribuído a um papel diferente.

```
CREATE USER joao WITH PASSWORD 'venda123';
CREATE USER maria WITH PASSWORD 'gerencia456';
CREATE USER pedro WITH PASSWORD 'admin789';
```

5 Atribuir Papéis aos Usuários

Execute os comandos para atribuir cada usuário ao seu respectivo papel. João → Vendedor, Maria → Gerente, Pedro → Admin.

```
GRANT vendedor TO joao;
GRANT gerente TO maria;
GRANT admin TO pedro;
```

6 Validação: Listar Papéis e Usuários Criados

Execute os comandos para verificar se todos os papéis e usuários foram criados com sucesso.

```
-- Listar papéis criados
SELECT rolname FROM pg_roles WHERE rolname IN ('vendedor', 'gerente', 'admin');

-- Listar usuários criados
SELECT usename FROM pg_user WHERE usename IN ('joao', 'maria', 'pedro');
```

Etapa 2: Concessão de Privilégios (GRANT)

PAPEL VENDEDOR

COMANDOS GRANT

```
GRANT SELECT ON produtos TO vendedor;
GRANT INSERT ON vendas TO vendedor;
```

JUSTIFICATIVA

Vendedor só pode ver produtos (SELECT) para consultar preço e estoque, e registrar novas vendas (INSERT). Não pode alterar, deletar ou criar nada.

PAPEL GERENTE

COMANDOS GRANT

```
GRANT SELECT ON produtos, vendas, funcionarios TO gerente;
GRANT INSERT, UPDATE ON produtos TO gerente;
GRANT INSERT, UPDATE ON vendas TO gerente;
```

JUSTIFICATIVA

Gerente pode consultar tudo (SELECT *) para relatórios, inserir e corrigir dados em Produtos e Vendas. Não pode deletar registros, fazer DROP ou ALTER (DDL).

PAPEL ADMIN

COMANDOS GRANT

```
GRANT ALL PRIVILEGES ON DATABASE northwind TO admin;
```

JUSTIFICATIVA

Admin tem controle total, incluindo DDL (CREATE, ALTER, DROP). Este é o papel mais crítico e deve ser atribuído apenas a DBAs confiáveis. Usar com extrema cautela.

Etapa 3: Testes de Acesso - Parte 1

👤 USUÁRIO: JOÃO (VENDEDOR)

1 Teste: Tentar UPDATE em Produtos

COMANDO:

```
UPDATE produtos SET preco = 100 WHERE id = 1;
```

❌ ERRO - Acesso Negado (Vendedor não tem UPDATE em Produtos)

2 Teste: Consultar Produtos

COMANDO:

```
SELECT * FROM produtos;
```

✓ SUCESSO - Vendedor pode consultar o catálogo de produtos

👔 USUÁRIO: MARIA (GERENTE)

3 Teste: Tentar DROP em Vendas

COMANDO:

```
DROP TABLE vendas;
```

❌ ERRO - Acesso Negado (Gerente não tem privilégios DDL)

4 Teste: Corrigir Erro de Venda

COMANDO:

```
UPDATE vendas SET valor = 50 WHERE id = 10;
```

✓ SUCESSO - Gerente pode corrigir erros de vendas

Etapa 3: Testes de Acesso - Parte 2

5 Pedro (Admin) - Criar Tabela (DDL)

COMANDO

```
CREATE TABLE auditoria (
  id INT PRIMARY KEY,
  usuario VARCHAR(50),
  acao VARCHAR(100),
  data_hora TIMESTAMP
);
```

✓ **RESULTADO ESPERADO: SUCESSO**

Admin pode criar tabelas (DDL). A tabela auditoria será criada com sucesso.

6 Pedro (Admin) - Deletar Tabela (DDL)

COMANDO

```
DROP TABLE auditoria;
```

✓ **RESULTADO ESPERADO: SUCESSO**

Admin pode deletar tabelas (DDL). A tabela auditoria será deletada com sucesso.

Resumo de Todos os Testes (1-6)

Teste	Usuário (Papel)	Comando	Resultado
1	João (Vendedor)	UPDATE produtos SET preco = 100	❌ ERRO
2	João (Vendedor)	SELECT * FROM produtos	✓ SUCESSO
3	Maria (Gerente)	DROP TABLE vendas	❌ ERRO
4	Maria (Gerente)	UPDATE vendas SET valor = 50	✓ SUCESSO
5	Pedro (Admin)	CREATE TABLE auditoria	✓ SUCESSO
6	Pedro (Admin)	DROP TABLE auditoria	✓ SUCESSO

Interpretação dos Resultados

Os testes confirmam que o RBAC foi implementado corretamente. Cada papel tem apenas os privilégios necessários: Vendedor não pode UPDATE, Gerente não pode DDL, Admin tem controle total. Erros esperados indicam que a segregação está funcionando.

Revogação de Privilégios (REVOKE)

⚠ **Mudança de Política**

A política da Northwind mudou. Agora o Gerente não pode mais inserir novos produtos, apenas visualizar e corrigir os existentes. Você precisa remover a permissão INSERT de Produtos do papel Gerente.

COMANDO REVOKE

```
-- Remover permissão INSERT de Produtos do papel Gerente
REVOKE INSERT ON produtos FROM gerente;
```

❌ Teste 1: Inserir Novo Produto (DEVE FALHAR)

COMANDO SQL

```
-- Logado como Maria (Gerente)
INSERT INTO produtos
  (id, nome, preco, estoque)
VALUES (999, 'Novo Produto', 50.00, 100);
```

❌ **ERRO: Acesso Negado (Permission denied)**

INTERPRETAÇÃO

A permissão INSERT foi revogada com sucesso. O Gerente não pode mais inserir novos produtos.

✓ Teste 2: Atualizar Produto Existente (DEVE FUNCIONAR)

COMANDO SQL

```
-- Logado como Maria (Gerente)
UPDATE produtos
SET preco = 75.00
WHERE id = 1;
```

✓ **SUCESSO: 1 linha atualizada**

INTERPRETAÇÃO

O Gerente ainda tem permissão UPDATE em Produtos. Pode corrigir dados existentes, mas não pode inserir novos.

Debate: Questões Críticas e Análise de Risco

Q1 **Qual foi o principal risco evitado ao negar a permissão DELETE ao papel Vendedor?**

RESPOSTA CHAVE

Evitar exclusão acidental ou intencional de registros de vendas, pedidos e histórico de transações. Isso destruiria a auditoria e a integridade dos dados financeiros da empresa.

ANÁLISE CRÍTICA

Um vendedor pode cometer erros ao digitar dados. Se tivesse DELETE, poderia apagar registros de vendas inteiras, causando perda de dados e inconsistências financeiras. O PoLP evita esse risco ao negar DELETE.

Q2 **Por que é um erro dar ALL PRIVILEGES a um usuário que é Cientista de Dados?**

RESPOSTA CHAVE

Um Cientista de Dados só precisa de SELECT nas camadas Prata/Ouro do Data Lake. Dar ALL PRIVILEGES viola o PoLP e expõe dados brutos (Bronze), estrutura do banco (DDL) e permite DELETE/DROP desnecessários.

ANÁLISE CRÍTICA

ALL PRIVILEGES inclui DDL (CREATE, ALTER, DROP) e DML perigoso (DELETE). Um Cientista de Dados não precisa deletar tabelas ou alterar estrutura. Isso aumenta o risco de erro catastrófico e viola conformidade (LGPD, HIPAA).

Q3 **Qual é o benefício de usar Papéis (Roles) em vez de atribuir privilégios diretamente a usuários individuais?**

RESPOSTA CHAVE

Administração centralizada: modificar privilégios de um papel afeta todos os usuários do papel automaticamente. Consistência: todos os vendedores têm exatamente os mesmos privilégios. Escalabilidade: novos usuários rapidamente.

ANÁLISE CRÍTICA

Com 500 usuários, gerenciar privilégios individuais é impossível e inconsistente. Com 5 papéis, é simples e auditável. Papéis também facilitam conformidade: você prova que todos os vendedores têm os mesmos privilégios, não mais, não menos.

Checklist de Validação e Auto-Avaliação

✓ CRIAÇÃO DE PAPÉIS E USUÁRIOS

- ☐ **ITEM 1**
  Criei os 3 papéis (vendedor, gerente, admin) com sucesso usando CREATE ROLE
- ☐ **ITEM 2**
  Criei os 3 usuários (João, Maria, Pedro) com senhas usando CREATE USER
- ☐ **ITEM 3**
  Atribuí cada usuário ao seu respectivo papel usando GRANT papel TO usuário

✓ CONCESSÃO DE PRIVILÉGIOS (GRANT)

- ☐ **ITEM 4**
  Concedi SELECT em Produtos e INSERT em Vendas ao papel Vendedor
- ☐ **ITEM 5**
  Concedi SELECT *, UPDATE/INSERT em Produtos e Vendas ao papel Gerente
- ☐ **ITEM 6**
  Concedi ALL PRIVILEGES ao papel Admin (incluindo DDL: DROP, ALTER, CREATE)

✓ TESTES DE ACESSO (VALIDAÇÃO)

- ☐ **ITEM 7**
  Testei que Vendedor NÃO pode UPDATE em Produtos (acesso negado com sucesso)
- ☐ **ITEM 8**
  Testei que Gerente NÃO pode DROP em Vendas (acesso negado com sucesso)

✓ COMPREENSÃO CONCEITUAL

- ☐ **ITEM 9**
  Entendo o Princípio do Menor Privilégio (PoLP) e sua importância para segurança
- ☐ **ITEM 10**
  Compreendo os benefícios de usar Papéis (Roles) em vez de gerenciar usuários individuais

Próximos Passos

Se você marcou todos os 10 itens, parabéns! Você implementou com sucesso uma estrutura RBAC completa. Se algum item não foi marcado, revise os comandos SQL e testes correspondentes antes de prosseguir.

Conclusão: Encerramento e Reflexão Final

RBAC É A FUNDAÇÃO DA SEGURANÇA DE DADOS

Você implementou com sucesso uma estrutura RBAC completa. Isso não é apenas um exercício técnico: é a base sobre a qual toda a segurança de dados de uma organização é construída. Sem RBAC, não há controle. Sem controle, não há segurança.

- RBAC separa responsabilidades e limita danos potenciais
- Facilita auditoria e conformidade regulatória (LGPD, HIPAA, SOX)
- Escala: gerenciar 5 papéis é mais simples que 500 usuários

SEGREGAÇÃO DE ACESSO POR FUNÇÃO

O Princípio do Menor Privilégio (PoLP) não é apenas uma boa prática: é a diferença entre um sistema seguro e um vulnerável. Cada papel deve ter apenas o que precisa, nada mais.

- Vendedor: SELECT + INSERT (não pode UPDATE, DELETE, DDL)
- Gerente: SELECT + UPDATE/INSERT (não pode DELETE, DDL)
- Admin: ALL PRIVILEGES (com grande responsabilidade)

Reflexão Final: Sua Responsabilidade como Profissional de Dados

Você agora sabe como implementar RBAC. Mas com esse conhecimento vem responsabilidade. Cada decisão de acesso que você toma afeta a segurança de dados pessoais, financeiros e de saúde de pessoas reais. Não é apenas código: é ética, conformidade e confiança.

Você é o Guardião da Segurança de Dados

Implemente RBAC com rigor. Segregue acesso com precisão. Audite com vigilância. A segurança de dados começa com você.