

# Melhorando sua postura de segurança no MySQL

Ronald Bradford Outubro de 2025

[https://ronaldbradford.com/presentations/  
me@ronaldbradford.com](https://ronaldbradford.com/presentations/me@ronaldbradford.com)



|                                                           |          |
|-----------------------------------------------------------|----------|
| <b>Agenda</b>                                             | <b>3</b> |
| <b>Sobre mim Autor   Palestrante   Colaborador</b>        | <b>3</b> |
| <b>O que é uma Postura de Segurança?</b>                  | <b>3</b> |
| <b>Por que isso é importante?</b>                         | <b>3</b> |
| <b>A segurança do banco de dados é a última defesa</b>    | <b>4</b> |
| <b>Avalie a saúde da segurança do seu banco de dados?</b> | <b>4</b> |
| <b>Verificações de Autoavaliação</b>                      | <b>5</b> |
| <b>Cinco (5) Passos Proativos</b>                         | <b>5</b> |
| <b>1. Rotação de Senhas</b>                               | <b>5</b> |
| <b>2. Use caching_sha2_password</b>                       | <b>6</b> |
| <b>2. Como usar - Usando caching_sha2_password</b>        | <b>6</b> |
| <b>3. Usando uma política de senhas mais forte</b>        | <b>6</b> |
| <b>3. Como usar uma política de senhas mais forte</b>     | <b>6</b> |
| <b>4. Limite o acesso SUPER e GRANT OPTION</b>            | <b>6</b> |
| <b>4. Como - Encontrar acesso SUPER</b>                   | <b>6</b> |
| <b>5. Use os novos recursos</b>                           | <b>7</b> |
| <b>NÃO FAÇA ISSO - Dias, não minutos</b>                  | <b>7</b> |
| <b>Arquiteturas de Referência do MySQL para Segurança</b> | <b>7</b> |
| <b>Segurança de Senhas 101</b>                            | <b>8</b> |
| <b>Conclusão</b>                                          | <b>8</b> |

**Peço desculpas, isso é traduzido automaticamente.**

# Agenda

- Por que a segurança é importante
- Classifique a segurança do seu MySQL agora
- Cinco etapas proativas para melhorar sua postura de segurança
- O que acontece quando você é exposto

## Sobre mim Autor | Palestrante | Colaborador

- 1999 - Comecei a usar MySQL (antes de 3.23) (26/30)
- 2006 - Primeira apresentação em conferência sobre MySQL (19/30)
- 2006 - 2008 Trabalhou na MySQL Inc.
- 2010 - 2017 Diretor Oracle ACE (Ex-aluno)
- 2025 - Diretor de Arquitetura de Banco de Dados - [VSCO](#)

## O que é uma Postura de Segurança?

A saúde geral da segurança cibernética de uma organização e sua prontidão para prevenir, detectar, responder e se recuperar de ameaças cibernéticas.

**"A segurança do seu banco de dados é a barreira final"**

## Por que isso é importante?

Não é um produto novo e brilhante. Não é um trabalho glamoroso. Mas, na realidade...

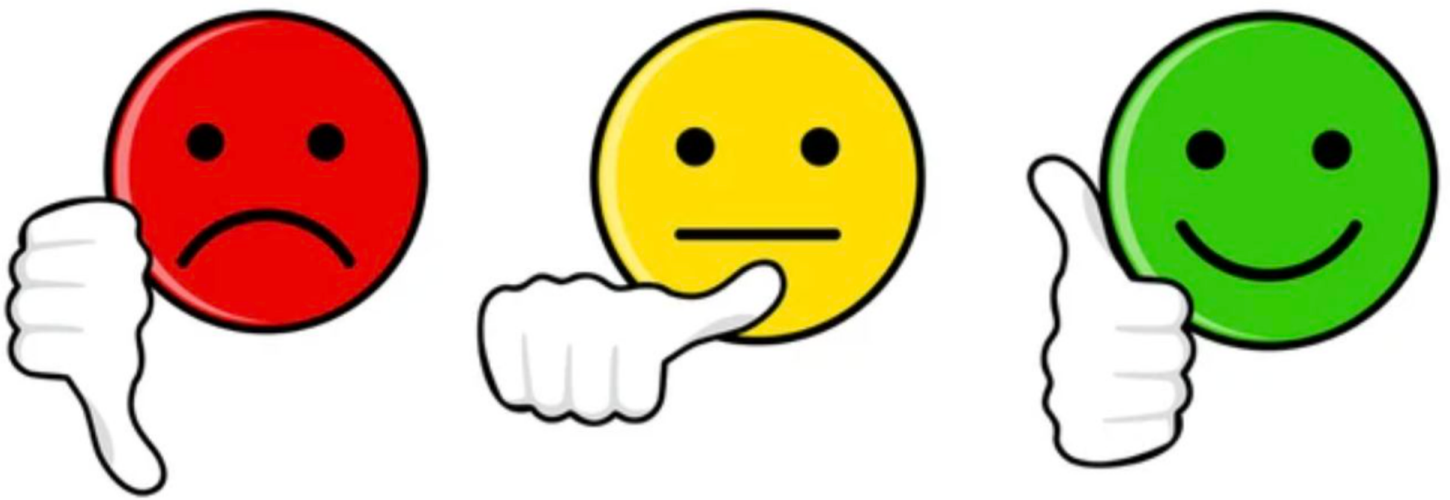
Se sua empresa fosse hackeada

e seus dados fossem roubados, você teria um emprego?

A segurança do banco de dados é a última defesa



Avalie a saúde da segurança do seu banco de dados?



# Verificações de Autoavaliação

- Contas sem senha
- Contas com senha fácil (arco-íris)
- Contas com autenticação insegura
- Contas com privilégio SUPER
- Contas com muitos privilégios
- Sem rotação de senha
- Contas não utilizadas
- Acesso a mysql.user
- Usando o usuário 'root' do MySQL
- Executar como usuário 'root' do SO
- Privilégios excessivos de data\_dir
- Acesso externo ao servidor
- Restringir acesso SUPER (servidor)
- Limitar acesso a recursos (SUPER)
- Sem TLS em trânsito
- Sem criptografia em repouso
- Senhas em texto simples (sistema de arquivos)
- Backups inseguros (não criptografados)
- Senhas padrão pesquisáveis
- Credenciais expostas (.env)

## Cinco (5) Passos Proativos

### 1. Rotação de Senhas

- Era difícil antes da versão 8.0
- É fácil a partir da versão 8.0
  - MANTER A SENHA ATUAL
  - DESCARTE A SENHA ANTIGA

## 2. Use caching\_sha2\_password

- O plugin mysql\_native\_password não é seguro
  - Veja a apresentação "RIP mysql\_native\_password"
- <https://speakerdeck.com/ronaldbradford/rip-mysql-native-password-2025-04>

## 2. Como usar - Usando caching\_sha2\_password

Aplicativo anterior ao MySQL 8.0 (disponível em 2018)

- Atualizar para o banco de dados MySQL 8.0 ◦ Continuar usando mysql\_native\_password
- Atualizar os conectores do cliente para versões compatíveis com versões 8.0 ou superiores ◦ Ou seja, ambos os plugins estão disponíveis
- Trocar usuários de mysql\_native\_password para caching\_sha2\_password
  - Idealmente, criar novos usuários (auditabilidade)
  - Usar PASSWORD EXPIRE para usuários antigos

## 3. Usando uma política de senhas mais forte

- Remova a possibilidade de usar senhas fáceis
- Não precisa ser com caracteres aleatórios
  - Ex.: Mercúrio-Vênus-Terra-Marte-2025

## 3. Como usar uma política de senhas mais forte

```
MOSTRAR VARIÁVEIS GLOBAIS COMO 'validate%';  
MOSTRAR STATUS COMO 'validate_password.%';  
DEFINIR GLOBAL validate_password.policy=STRONG;  
DEFINIR GLOBAL validate_password.length=16;
```

## 4. Limite o acesso SUPER e GRANT OPTION

- Sem usuários genéricos
- Limite os hosts a partir dos quais eles podem se conectar
- Limite conexões simultâneas (MAX\_USER\_CONNECTIONS)
- Limite de consultas por hora (MAX\_QUERIES\_PER\_HOUR)
- Altere o padrão de "root" para outro usuário
- Bloqueie senhas inválidas

## 4. Como - Encontrar acesso SUPER

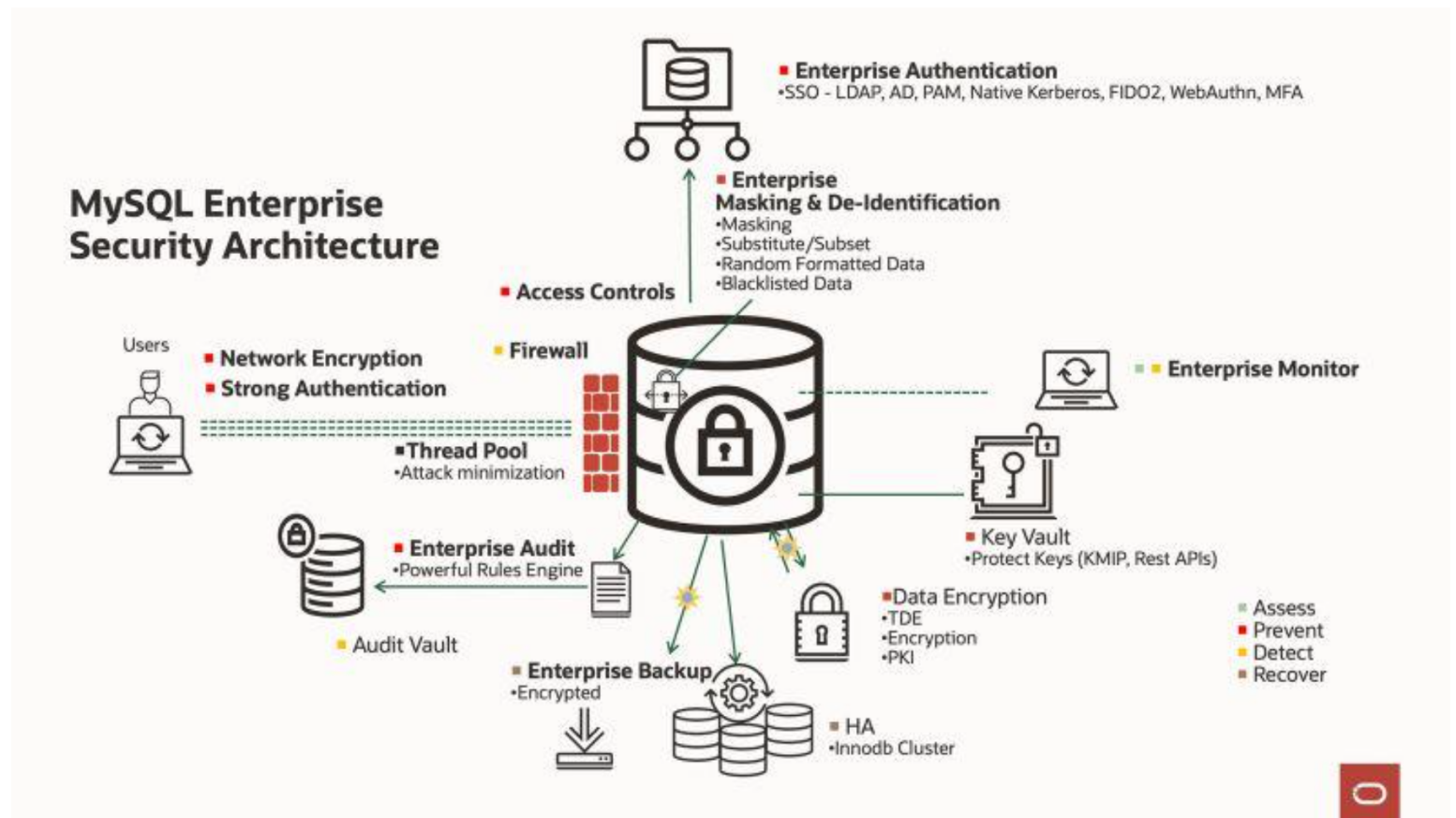
Banir TODOS

## 5. Use os novos recursos

- Expira senhas importantes (consulte INTERVALO DE EXPIRAÇÃO 'n' DIA)
- TLS/SSL (consulte EXIGIR SSL)
- Desativar o uso de senhas antigas (consulte HISTÓRICO DE SENHAS 'n')
- Bloquear contas em caso de falha (consulte TENTATIVAS\_DE\_LOGIN\_FALHAS 'n')
- MFA - Complicado

NÃO FAÇA ISSO - Dias, não minutos

## Arquiteturas de Referência do MySQL para Segurança



<https://www.mysql.com/why-mysql/white-papers/mysql-reference-architectures-for-security/>

# Segurança de Senhas 101

- Use regras de autenticação mais fortes
- Use a autorização com privilégios mínimos
- Usuário individual por serviço, produto, ferramenta, monitoramento
- Migração para um gerenciamento de usuários centralizado e baseado em tokens
  - Elo mais fraco - Credenciais em texto simples (em arquivos)

<https://dev.mysql.com/doc/refman/9.3/en/create-user.html>

## Conclusão

- FÁCIL - Faça o mínimo para os aplicativos
- MENOS FÁCIL - Atualizando os usuários do banco de dados
  - Novo processo de administração
- DIFÍCIL - Substituindo todos os conectores do cliente
- DIFÍCIL - Controles proativos

O que é mais importante?

Trabalho DIFÍCIL ou ser HACKEADO