ORAMASTER

Criptografando Dados com TDE no Oracle Database


DBA BRASIL
DATA & CLOUD
Diamante
AGGRANDIZE
COMMVAULT
TD SYNNEX
Platina
GOLDENGATEBR
Consultoria & Treinamentos
DISCOVER
Ouro
scansource
VERTICA
by opentext
Prata
TRACES
CAFÉ
COM
CLOUD
Rox
We take care
of your data
Apoio
FIAP
GRUPO
POSEIDON
DIGITAL

APRESENTAÇÃO DO PALESTRANTE

QUEM SOU EU?

https://www.linkedin.com/in/dbafabioprado/

QUEM SOU EU?

- Trajetória profissional:
  - ✓ Cargos administrativos: 1992-2001
  - ✓ Analista de Suporte: 2001-2002
  - ✓ **Desenvolvedor**: 2002-2007
  - ✓ **DBA**: 2007...
  - ✓ **Instrutor/Professor**: 2009…
- Experiência de **22 anos** em TI, em diversas empresas da área pública e privada, de diversos ramos de atuação;
- Ministrei treinamentos oficiais Oracle na KaSolution e IBTA;
- Fui professor de pós-graduação em disciplinas relacionadas a banco de dados na IBTA e UNICAMP.

QUEM SOU EU?

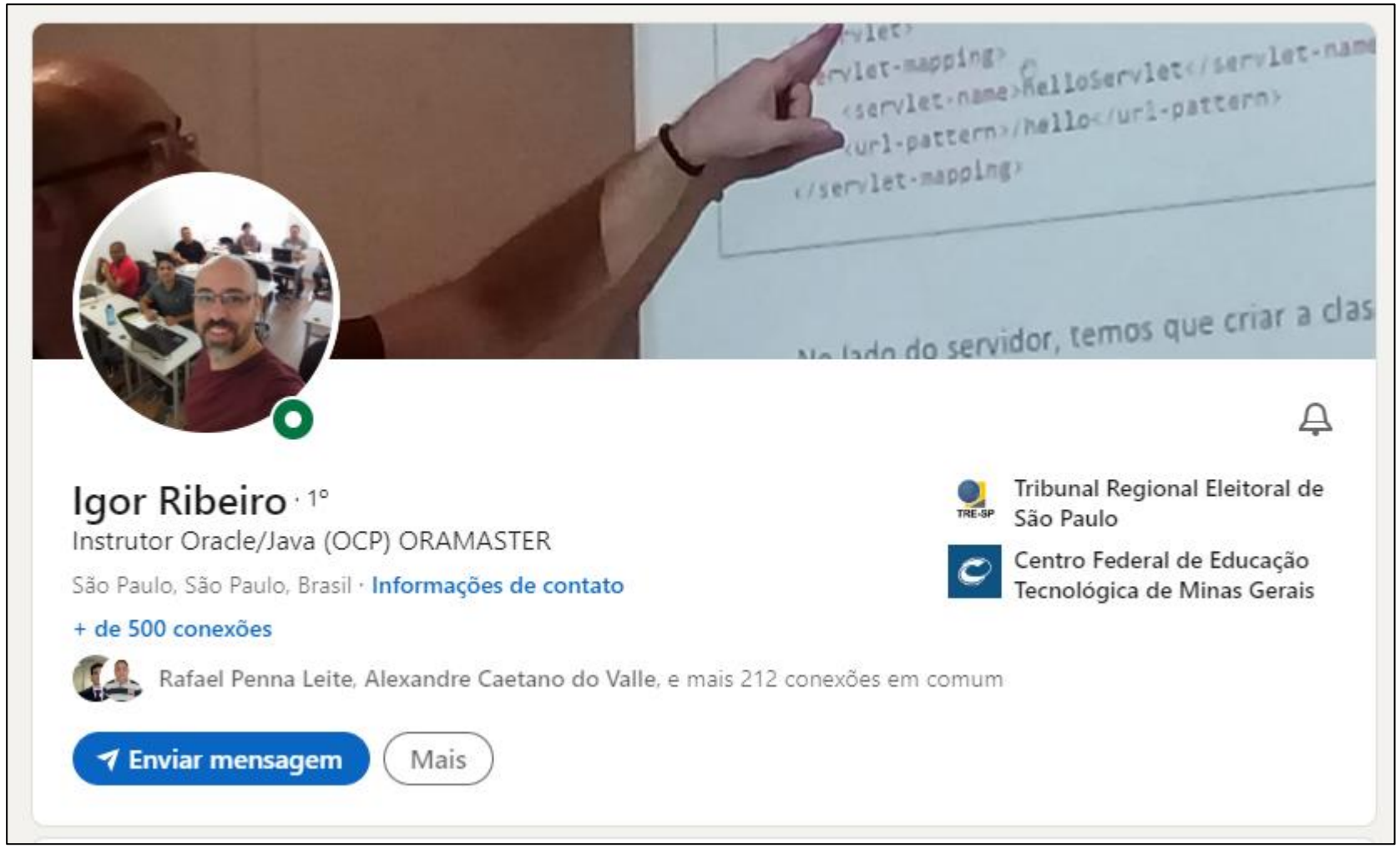
- Atualmente ministro treinamentos Oracle somente na **Oramaster.**
- Bacharel em Ciências da Computação, com MBA e Pós-graduação em Gestão de Projetos;
- Autor do blog FABIOPRADO.NET;
- Fui Organizador do **DBA BRASIL**;
- Fui articulista da revista *SQL Magazine* e diversos sites e blogs de TI, tais como: OTN (Oracle Technology Network), GPO (Grupo de Profissionais Oracle), Portal GSTI, TI Especialistas, DevMedia e ProfissionaisTI.

CERTIFICAÇÕES E TÍTULOS

- Oracle:
  - Oracle ACE;
  - Oracle Certified Expert, Oracle DB 11g Release 2 SQL Tuning ;
  - Oracle Database 11g Performance Tuning Certified Expert;
  - Oracle Certified Professional (OCP) Database 10G / 11G / 12c;
  - Oracle PL/SQL Developer Certified Associate 11G;
  - OCI 2019 Architect Associate;
  - Oracle Autonomous Database Specialist;
  - OCI Foundations 2020 Associate: 04/2020

- Microsoft:
  - MCP, MCSD, MCAD, MCSD.NET, MCDBA, MCTS, MCT e MCPD.

QUEM É ELE?



https://www.linkedin.com/in/igorribeirodba/

Criptografando Dados com TDE no Oracle Database

PRÉ-REQUISITOS

- Ter conhecimentos básicos da arquitetura do Oracle DB;
- Desejável ter experiência como DBA. DBAs (ou profissionais com conhecimentos similares em BD) conseguirão apreender melhor o conteúdo!

AGENDA

- Apresentar uma visão geral do Oracle TDE, suas principais características e como implementar TDE no nível dos tablespaces;
- Incluso hands-on para aplicar os conhecimentos apresentados!

O que é TDE?

VISÃO GERAL

- Transparent Data Encryption (TDE) é uma “feature” que nasceu no Oracle 10GR2 e que possibilita criptografar dados no Oracle DB;
- Permite proteger dados confidenciais de **colunas e tablespaces**, criptografando os dados e armazenando-os fisicamente de modo seguro, possibilitando evitar roubo de dados diretamente nos datafiles gravados no SO;
- Aos consultar estes dados (criptografados), eles são **descriptografados** antes de serem apresentados para o usuário final;
- A criptografia e descriptografia dos dados ocorre de forma **transparente**, sem a necessidade de escrever linhas de código adicionais na aplicação ou no banco de dados.

VISÃO GERAL

- Uma chave de criptografia é armazenada no Dicionário de Dados e ela é utilizada para posterior descriptografia;
- A chave de criptografia utilizada no Banco de Dados também é criptografada por outra chave, que é chamada de **chave mestra** e é armazenada fora do BD, em um local seguro chamado keystore;
- Nos dados, antes da criptografia, são adicionadas palavras extras chamadas **SALT,** que alteram os dados originais e que ajudam a dificultar "ataques hackers" de descriptografia. SALT é adicionado por padrão no TDE e é obrigatório no nível dos tablespaces;
- Os dados podem ser criptografados utilizando um dos seguintes algoritmos: ARIA128, ARIA192, ARIA256, GOST256, SEED128, *3DES168*, ***AES128*** *(default para TDE tablespace)*, ***AES192*** *(default para TDE column)* e AES256.

OVERHEAD COM TDE

O impacto na performance depende do workload do BD e da plataforma. Muitas CPUs modernas fornecem aceleração de hardware embutidas, resultando em mínimo impacto na performance.

What is the overhead associated with TDE?

	TDE tablespace encryption (Oracle Database 11g+)
Storage	No additional storage overhead.
Performance	According to internal benchmarks and feedback from our customers running production workloads, the performance overhead is typically in the single digits. Starting with Oracle Database 11g Release 2 Patchset 1 (11.2.0.2), the hardware crypto acceleration based on AES-NI available in recent Intel processors is automatically leveraged by TDE tablespace encryption, making TDE tablespace encryption a 'near-zero impact' encryption solution.

Shall I use TDE column encryption or TDE tablespace encryption?

Our recommendation is to use TDE tablespace encryption. TDE tablespace encryption has better, more consistent performance characteristics in most cases. Moreover, tablespace encryption in particular leverages hardware-based crypto acceleration where it is available, minimizing the performance impact even further to the 'near-zero' range. Support for hardware-based crypto accelaration is available since Oracle Database 11g Release 2 Patchset 1 (11.2.0.2) for Intel chipsets with AES-NI and modern Oracle SPARC processors.

For more details on TDE column encryption specific to your Oracle Database version, please see the Advanced Security Guide under Security on the Oracle Database product documentation that is available here.

LICENCIAMENTO

How is TDE licensed?

TDE is part of the Oracle Advanced Security, which also includes Data Redaction. It is available as an additional licensed option for the Oracle Database Enterprise Edition. In Oracle Autonomous Databases and Database Cloud Services it is included, configured, and enabled by default.

Section I — **Prices in USA (Dollar)**

	Oracle Database			
	Named User Plus	Software Update License & Support	Processor License	Software Update License & Support
Database Products				
Oracle Database				
Standard Edition 2	350	77.00	17,500	3,850.00
Enterprise Edition	950	209.00	47,500	10,450.00
Personal Edition	460	101.20	-	-
Mobile Server	-	-	23,000	5,060.00
NoSQL Database Enterprise Edition	200	44	10,000	2,200.00
Enterprise Edition Options:				
Multitenant	350	77.00	17,500	3,850.00
Real Application Clusters	460	101.20	23,000	5,060.00
Real Application Clusters One Node	200	44.00	10,000	2,200.00
Active Data Guard	230	50.60	11,500	2,530.00
Partitioning	230	50.60	11,500	2,530.00
Real Application Testing	230	50.60	11,500	2,530.00
Advanced Compression	230	50.60	11,500	2,530.00
Advanced Security	300	66.00	15,000	3,300.00
Label Security	230	50.60	11,500	2,530.00
Database Vault	230	50.60	11,500	2,530.00
OLAP	460	101.20	23,000	5,060.00
TimesTen Application-Tier Database Cache	460	101.20	23,000	5,060.00
Database In-Memory	460	101.20	23,000	5,060.00
Database Enterprise Management				
Diagnostics Pack	150	33.00	7,500	1,650.00
Tuning Pack	100	22.00	5,000	1,100.00
Database Lifecycle Management Pack	240	52.80	12,000	2,640.00
Data Masking and Subsetting Pack	230	50.60	11,500	2,530.00
Cloud Management Pack for Oracle Database	150	33.00	7,500	1,650.00

Características gerais do TDE

CONSIDERAÇÕES E CARACTERÍSTICAS GERAIS

- Dados de colunas permanecem criptografados nos datafiles, undo, redo logs e Buffer Cache, mas é possível vê-los em “texto claro” em arquivos de swap, por esse motivo os privilégios de SO nestes tipos de arquivos devem ser muito bem gerenciados;

- Habilitar TDE em uma tabela resulta em um “full table update”, por isso cuidado ao executar este procedimento em uma tabela grande, pois poderá ocorrer um grande impacto de escrita nos redo logs e a tabela poderá ficar temporariamente indisponível para DMLs;

- Dados de UNDO e metadados do TEMP gerados a partir de dados criptografados em tablespaces são automaticamente criptografados também, por isso, criptografar os tablespaces de UNDO e TEMP é opcional;

CONSIDERAÇÕES E CARACTERÍSTICAS GERAIS

- A Oracle recomenda criptografar os tablespaces de sistema usando o algoritmo default **AES128;**
- Novos dados inseridos em tablespaces JÁ criptografados serão automaticamente criptografados;
- Dados criptografados necessitam de maior espaço de armazenamento, devido ao SALT e PADDING;
- O keystore pode ser armazenado no **Oracle Wallet** (ASM, Oracle ACFS ou SO), no **Oracle Key Vault** ou no OCI KMS;
- Os tablespaces podem ser criptografados em modo online (maior disponibilidade, a partir do Oracle 12.2) ou offline (menor consumo de storage). SYSTEM e UNDO não podem ser criptografados no modo offline.

CONSIDERAÇÕES E CARACTERÍSTICAS GERAIS

- Se o UNDO tablespace for criptografado a Oracle não recomenda descriptografá-lo depois;
- É possível fazer criptografia de tablespaces de usuário em paralelo, executando o procedimento em sessões diferentes. Não criptografe o SYSTEM e UNDO concorrentemente com outros tablespaces;
- Os tablespaces de sistema (SYSTEM, SYSAUX, TEMP e UNDO) estarão sempre disponíveis, mesmo com o keystore fechado;
- Se o keystore estiver fechado, operações de leitura/escrita nos tablespaces de usuário irão falhar com o erro "*ORA-2835 wallet is not open*" nas versões mais recentes do Oracle;

CONSIDERAÇÕES E CARACTERÍSTICAS GERAIS

- TDE no nível dos tablespaces criptografa/descriptografa os dados durante as operações de leitura/escrita, enquanto que, TDE no nível das colunas criptografa/descriptografa os dados na camada de SQL. Isso impõe diversas restrições que não existem no nível dos tablespaces, tais como:
  - Não criptografar alguns tipos dados (Ex.: LOB);
  - Não criptografar alguns tipos de índices.
- Por questões de segurança, é obrigatório o uso de SALT ao criptografar tablespaces;
- É possível mudar o algoritmo de criptografia padrão dos tablespaces através do parâmetro TABLESPACE_ENCRYPTION_DEFAULT_ALGORITHM;
- Recomenda-se configurar o parâmetro ENCRYPT_NEW_TABLESPACES p/ permitir que novos tablespaces sejam criptografados automaticamente.

CONSIDERAÇÕES E CARACTERÍSTICAS GERAIS

- Undo e metadados do TEMP gerados a partir de dados criptografados em tablespaces são automaticamente criptografados também, por isso, criptografar os tablespaces de UNDO e TEMP é opcional.

Implementando TDE no nível dos tablespaces

PRIVILÉGIOS NECESSÁRIOS

- É necessário ter os privilégios administrativos:
  - SYSKM;
  - ADMINISTER KEY MANAGEMENT.

KEYSTORE MODE: UNITED X ISOLATED

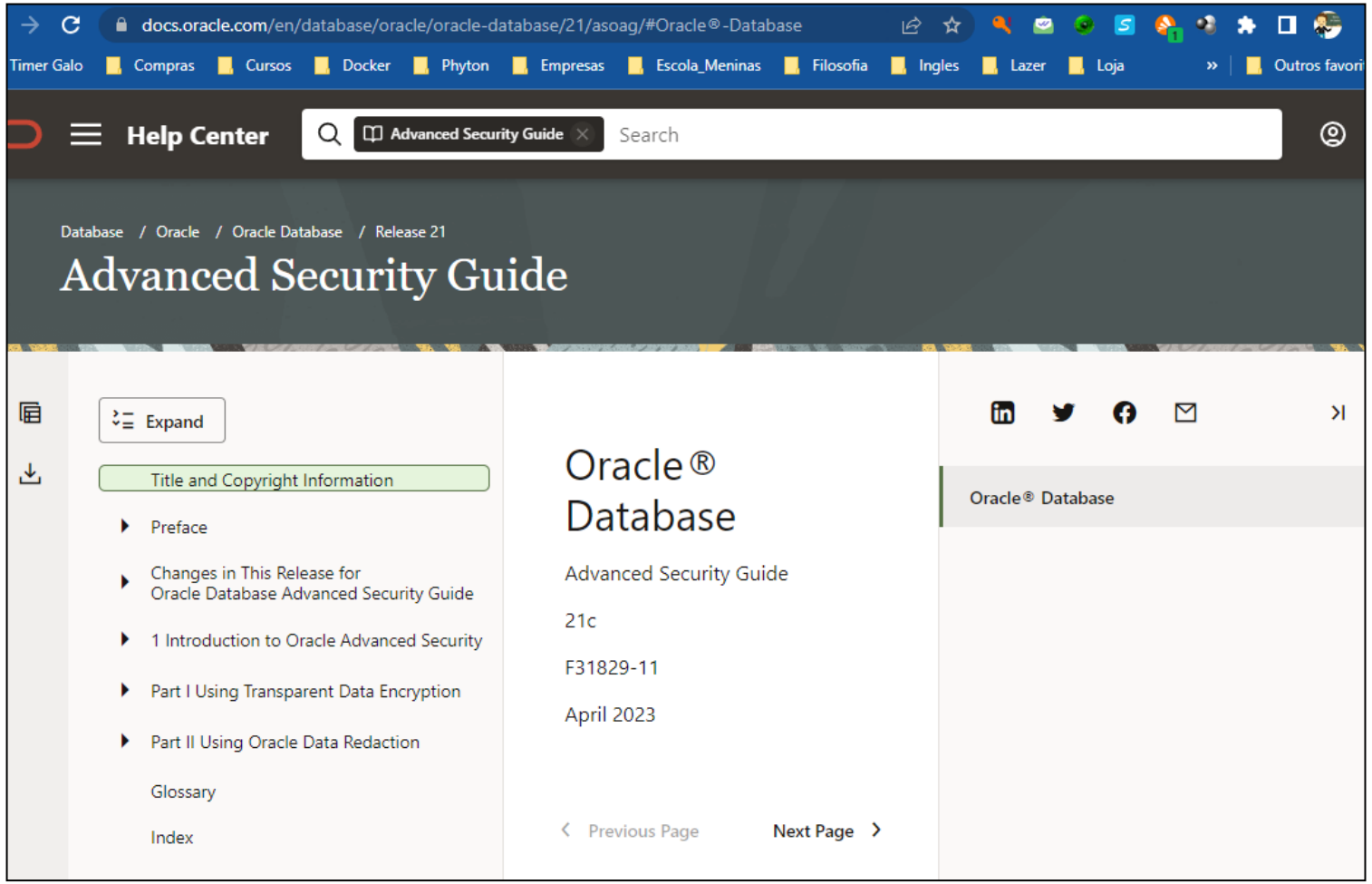
- **United** keystore mode (default):
  - O “container root” tem um keystore que é compartilhado com todos os PDBs do mesmo container;
  - Cada PDB tem sua chave de criptografia, mas todas armazenadas no mesmo keystore;
  - Mais fácil de gerenciar.
- **Isolated** keystore mode:
  - Disponível a partir do Oracle 19.11;
  - Cada PDB tem seu próprio keystore;
  - Maior segurança e mais flexibilidade (os PDBs podem ter keystores de tipos diferentes);
  - Mais keystores para gerenciar e proteger;
  - Possibilita melhor performance em operações de “rekey”.

PASSO A PASSO

1. Crie/configure um keystore;
2. Create uma master key inicial;
3. Configure auto-login no keystore;
4. Criptografe os tablespaces usando comandos SQL (ou o EM 12c ou versão superior).

PARTE FINAL

APRENDA MAIS



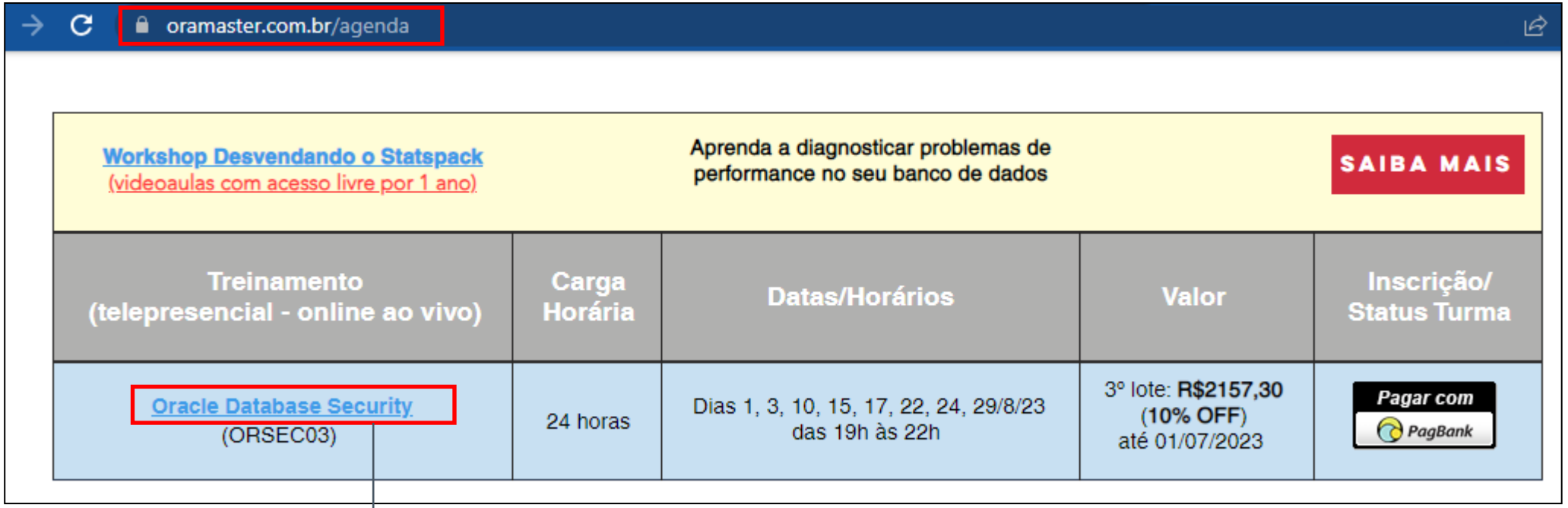
HORA DA FOTO

SORTEIO E VOUCHERS

- **50% OFF** para todos que tiverem interesse em participar da próxima turma do treinamento “**Oracle Database Security**”;

- **100% OFF** para um participante que será sorteado (https://www.random.org/) e que poderá escolher um dos treinamentos abaixo:
  - Administração;
  - Backup and Recovery;
  - Oracle SQL Tuning;
  - Oracle Database Tuning;
  - Oracle Database Security;
  - Oracle Data Guard;
  - Videoaulas de SQL ou PL/SQL.

SORTEIO E VOUCHERS



Clique aqui para ver o conteúdo programático do treinamento

REFERÊNCIAS

- Transparent Data Encryption FAQ, acessado em 14/6/2023
- Advanced Security Guide 21c, F31829-11, April 2023


That's all Folks!
contato@fabioprado.net