

UNIVERSIDADE REGIONAL DE BLUMENAU
CURSO DE SISTEMAS DE INFORMAÇÃO



SISTEMA PARA AUDITORIA DE SEGURANÇA DE BANCO DE DADOS ORACLE.

Alan Filipe Mattiollo

Prof. Cláudio Ratke, Orientador

ROTEIRO DA APRESENTAÇÃO

- Introdução
- Objetivos
- Fundamentação teórica
- Desenvolvimento e especificações do sistema
- Operacionalidade do sistema
- Resultados e discussões
- Conclusão
- Extensões
- Referências



INTRODUÇÃO

- A necessidade de informatizar o negócio e armazenar as informações para posterior utilização, considerando a necessidade de se ter fácil acesso a estas informações, cria um grande desafio no campo de segurança da informação;
- O RDBMS Oracle contém uma vasta quantidade de funções relacionadas a segurança, muitas são desconhecidas ou não são utilizadas corretamente;
- Necessidade de um processo de auditoria de conformidade através da utilização de um manual de regras bem definido.



OBJETIVOS

Desenvolver um sistema que verifique o nível de segurança de um banco de dados Oracle, visando facilitar a análise das alterações necessárias para que o ambiente em questão se torne mais seguro.

- Manter parâmetros e recursos de segurança para posterior verificação de conformidade;
- Emitir relatórios que informem as inconformidades de segurança da base de dados e os valores das configurações que precisam ser ajustadas para que se adequem ao modelo de segurança escolhido;
- Permitir a análise de verificações anteriores, mantendo um histórico para consulta.



FUNDAMENTAÇÃO TEÓRICA

Arquitetura do banco de dados Oracle

Uma instância Oracle compreende uma área de memória chamada SGA e processos de segundo plano (LONEY, 2009).

O Oracle é projetado para ser um banco de dados bastante portátil, a arquitetura física é diferente em diferentes sistemas operacionais (KYTE, 2010).

O dicionário de dados é um conjunto de metadados: dados sobre dados (WATSON, 2010).



Common Criteria

O *Common Criteria* é um padrão internacional para certificação de segurança de produtos de tecnologia da informação.

- Os produtos são avaliados por laboratórios independentes e licenciados;
- Documentos de suporte são utilizados durante a avaliação;

Um grupo de critérios com padrões técnicos é qualificado como modelo de proteção (WALLACE, 2003).

O Oracle Database 11g Release 2 Enterprise Edition é certificado.



Auditoria

A auditoria é um exame metódico ou revisão de um ambiente que tem por objetivo garantir complacência com regulamentos e detectar anomalias (CHAPPLE; STEWART; TITTEL, 2005).

É preciso monitorar o uso de privilégios que podem ser perigosos (BRYLA; RAMKLASS; WATSON, 2010).



Segurança em banco de dados Oracle

O princípio mais seguro a seguir quando determinar o acesso aos sistemas de computador é o do menor privilégio: ninguém pode ter acesso a qualquer coisa que esteja além do mínimo absolutamente necessário para executar seu trabalho, e qualquer coisa não especificamente permitida é proibida (WATSON, 2010).

Os mecanismos de segurança fornecidos pela Oracle dividem-se em três categorias: autenticação, autorização e auditoria (BRYLA; LONEY, 2009).

Oracle Listener.



Autenticação de banco de dados

No processo de autenticação, o método de identificação mais utilizado é o de usuário e senha (NATAN, 2005).



Fonte: Natan (2005).

Autorização

A autorização no Oracle é baseada em um modelo de privilégio, através do qual podem ser permitidos ou negados acessos a dados, ações ou processamento, e através do qual podem ser aplicados vários limites em tais ações ou acessos (NATAN, 2009).

Cenário Atual

A necessidade de verificar as configurações relacionadas à segurança é uma demanda anual de um cliente da Teclógica.

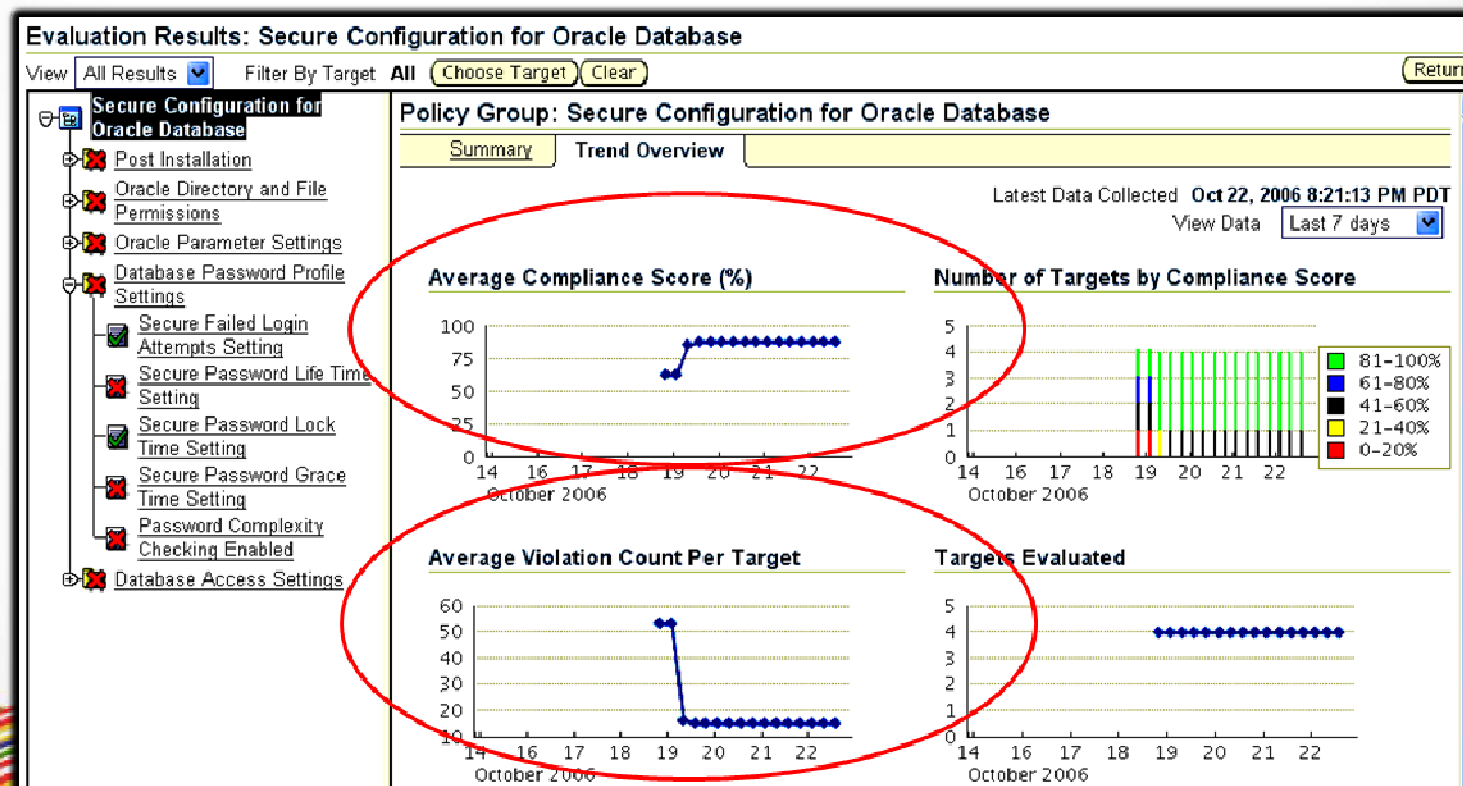
Toda a análise realizada para certificar-se de que o banco de dados alvo atende a todos os requisitos é feita manualmente, item a item.

É preciso avaliar o resultado de determinado requisito no ambiente e compará-lo ao valor esperado no documento que descreve o modelo de segurança da empresa.



Trabalhos Correlatos

O software correlato Oracle Enterprise Manager Configuration Management Pack (CMP), monitora as configurações do banco de dados para complacência em segurança e regulamentações. O CMP avalia continuamente as configurações, usando uma biblioteca de mais de 240 melhores práticas. A pontuação de complacência é calculada com base em políticas pré-definidas e configurações validadas por padrões industriais, como o Center for Internet Security (CIS).



DESENVOLVIMENTO E ESPECIFICAÇÕES DO SISTEMA

Requisitos Funcionais

Manter:

- Configurações de *profile*;
- Grupos de privilégios;
- Privilégios de sistema;
- Comandos auditáveis;
- Parâmetros do *SQLNet*;
- Parâmetros de instância;
- Parâmetros do *Listener*;
- Contas de usuário.

Criar e Excluir:

- Modelos de segurança.

Verificar:

- Banco de dados alvo.

Visualizar:

- Resultados da análise do banco de dados;
- Resumo dos itens verificados.

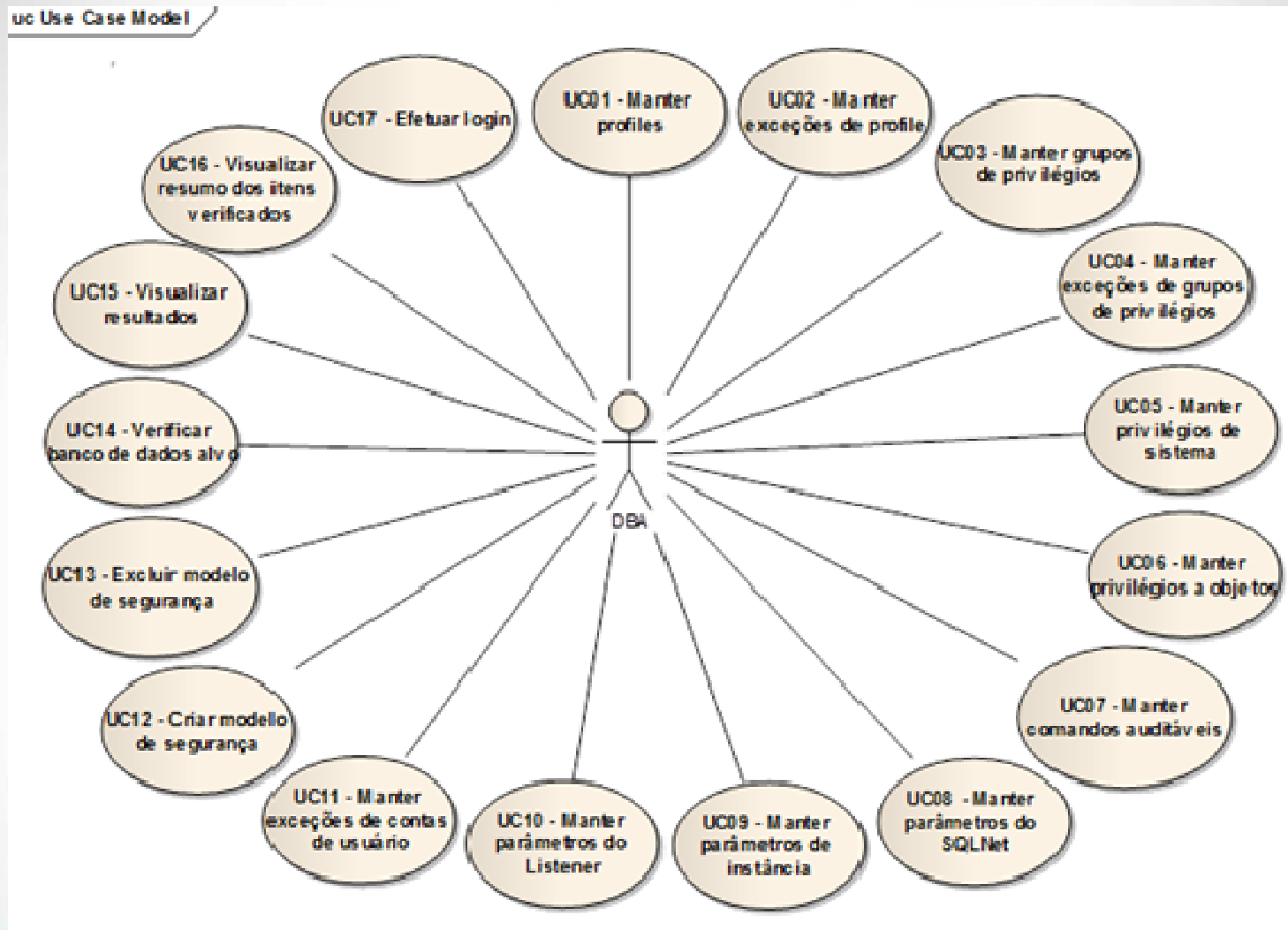


Requisitos Não Funcionais

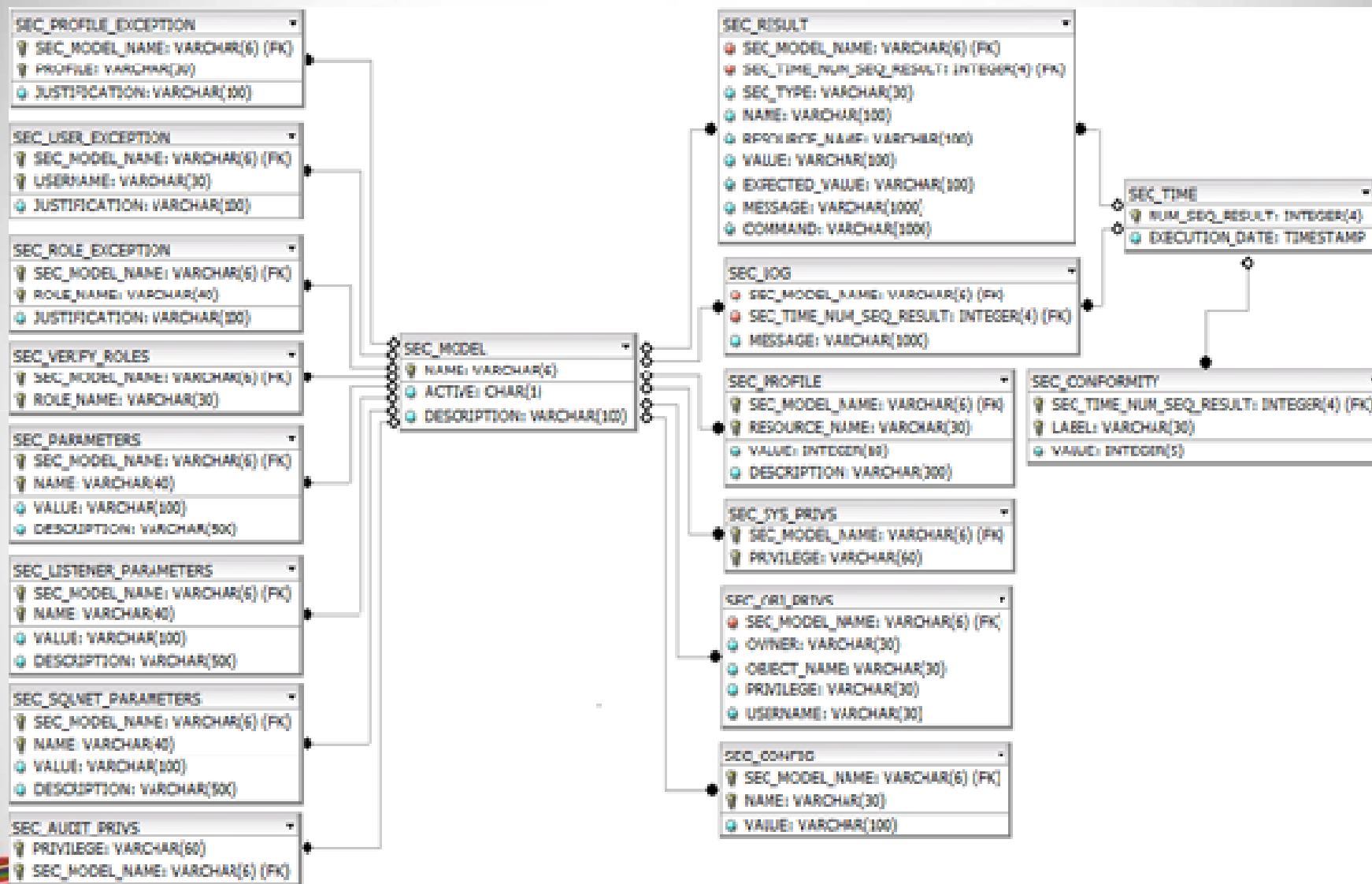
- O sistema deverá utilizar banco de dados Oracle 11g (portabilidade);
- O sistema será desenvolvido em PL/SQL (implementação);
- As páginas e relatórios serão desenvolvidos através do Oracle APEX (implementação);
- O sistema poderá ser acessado através de qualquer navegador (portabilidade).



Diagrama de Caso de Uso



Modelo de Entidade e Relacionamento



Técnicas e Ferramentas Utilizadas

Ferramentas de desenvolvimento:

- SQL Developer;
- Application Builder (Oracle Application Express).

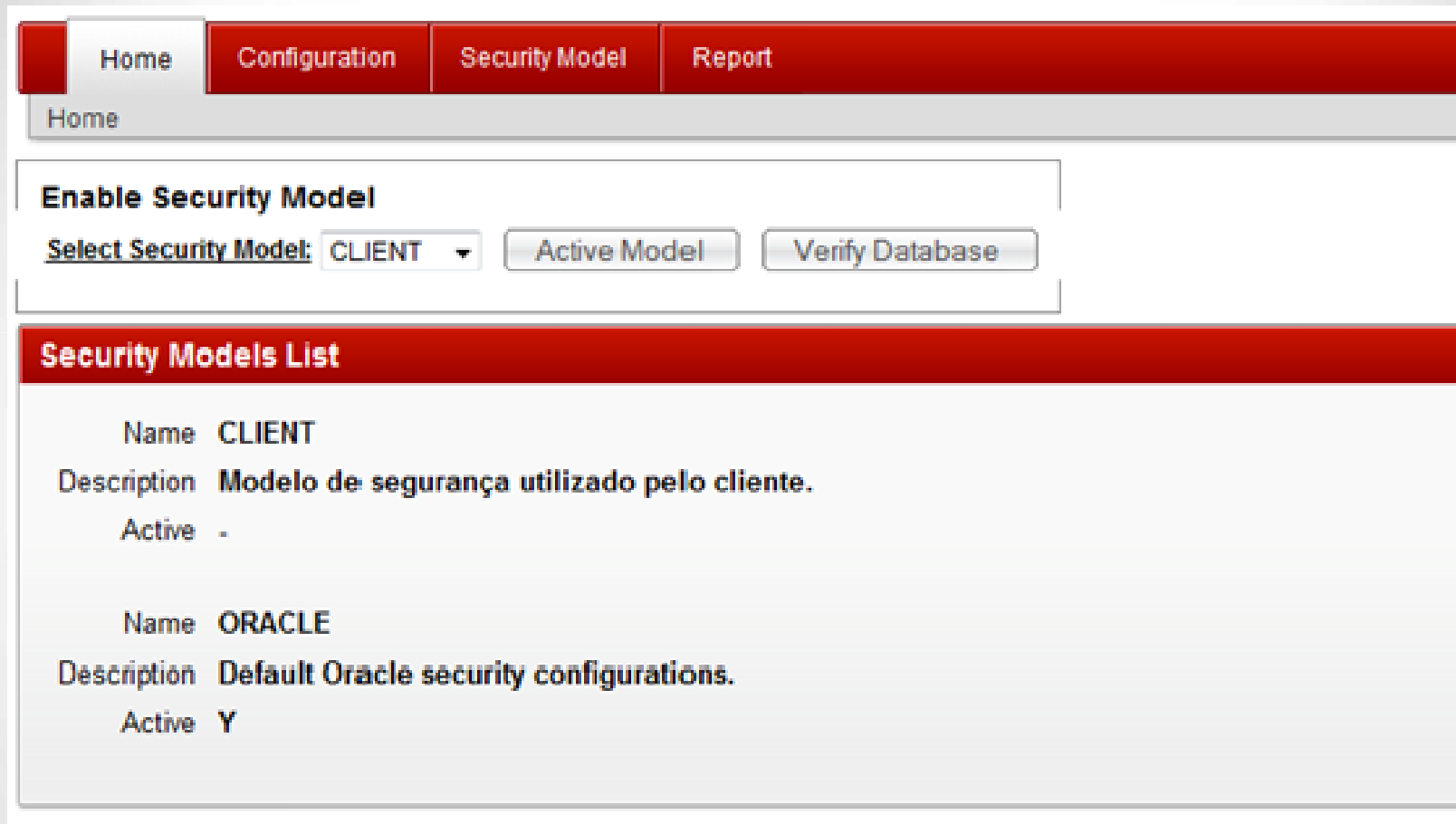
Banco de dados: Oracle Database 11g Enterprise Edition Release 2.

Servidor *web*: Oracle Weblogic 11g.



OPERACIONALIDADE DA IMPLEMENTAÇÃO

Página inicial do sistema



The screenshot displays the initial page of a system. At the top, there is a navigation bar with four tabs: Home, Configuration, Security Model, and Report. The 'Home' tab is currently selected. Below the navigation bar, there is a section titled 'Enable Security Model'. This section contains a dropdown menu labeled 'Select Security Model' with 'CLIENT' selected, and two buttons: 'Active Model' and 'Verify Database'. Below this section is a red header for 'Security Models List'. The list contains two entries:

Name	CLIENT
Description	Modelo de segurança utilizado pelo cliente.
Active	-
Name	ORACLE
Description	Default Oracle security configurations.
Active	Y

Página de criação e exclusão de modelo de segurança

Home	Configuration	Security Model	Report
------	---------------	----------------	--------

Home > Security Model

Create New Security Model

Model Name:

Description:

66 of 100

Template:

Delete Security Model

Select Security Model:

Warning: Default or active security models cannot be deleted. The exclusion of the security model will erase your entire history checks.



Página principal de configuração

Home Configuration Security Model Report

Home > Configuration

SEC Configuration

* Listener Directory: C:\app\oracle\product\11.2.0\dbhome_1\NETWORKADMIN

Security Model Options

- Profiles
- Roles
- System Privileges
- Object Privileges
- Audit Command
- SQLNet Parameters
- Instance Parameters
- Listener Parameters

Exception Users

<input type="checkbox"/>	Model Name	Username	Justification
<input type="checkbox"/>	ORACLE	ANONYMOUS	Predefined Oracle Database Administrative User Account
<input type="checkbox"/>	ORACLE	APEX_PUBLIC_USER	Predefined Oracle Database Non-Administrative User Account
<input type="checkbox"/>	ORACLE	CTXSYS	Predefined Oracle Database Administrative User Account
<input type="checkbox"/>	ORACLE	DBSNMP	Predefined Oracle Database Administrative User Account
<input type="checkbox"/>	ORACLE	DIP	Predefined Oracle Database Non-Administrative User Account
<input type="checkbox"/>	ORACLE	EXFSYS	Predefined Oracle Database Administrative User Account
<input type="checkbox"/>	ORACLE	FLWS_30000	Predefined Oracle Database Non-Administrative User Account
<input type="checkbox"/>	ORACLE	FLWS_FILES	Predefined Oracle Database Non-Administrative User Account
<input type="checkbox"/>	ORACLE	LBACSYS	Predefined Oracle Database Administrative User Account
<input type="checkbox"/>	ORACLE	MDDATA	Predefined Oracle Database Non-Administrative User Account

Download

row(s) 1 - 10 of 30



Página de configuração de *profiles* de conta de usuário

Home Configuration Security Model Report

Home > Configuration > Profile

Exception Profiles

Cancel Create

Model Name: ORACLE
Profile: APEX
Justification:
View Profile Exceptions

Profile Settings

Cancel Delete Submit

<input type="checkbox"/>	Model Name	Resource Name	Value	Description
<input type="checkbox"/>	ORACLE	failed_login_attempts	3	Restricting the number of login attempts will help deter brute force attacks against profiles.
<input type="checkbox"/>	ORACLE	password_grace_time	3	Specified in days the amount of time that the user is warned to change their password before their password expires.
<input type="checkbox"/>	ORACLE	password_life_time	90	Restricting the password lifetime will help deter brute force attacks against user accounts and refresh passwords.
<input type="checkbox"/>	ORACLE	password_lock_time	1	Specifies the amount of time in days that the account will be locked out if the maximum number of authentication attempts has been reached.
<input type="checkbox"/>	ORACLE	password_reuse_max	20	This prevents users from cycling through a few common passwords and helps ensure the integrity and strength of user credentials.
<input type="checkbox"/>	ORACLE	password_reuse_time	365	Creating a long window before password reuse helps protect from password brute force attacks and helps the strength and integrity of the user credential.

Download

Add Row

Home Configuration Security Model Report

Home > Configuration > Profile > Profile Exceptions

Configure Profile Exceptions

Cancel Delete Submit

<input type="checkbox"/>	Model Name	Profile	Justification
<input type="checkbox"/>	ORACLE	APEX	Profile de aplicação.

1-1

Add Row

Página de configurações de *roles*

Home Configuration **Security Model** Report

Home > Configuration > Roles

Exception Roles Cancel Create

Model Name: ORACLE ▾

Role Name: ADM_PARALLEL_EXECUTE_TASK ▾

Justification

View Role Exceptions

Configure Roles Cancel Delete Submit

<input type="checkbox"/>	Model Name	Role Name ▾
<input type="checkbox"/>	ORACLE	CONNECT
<input type="checkbox"/>	ORACLE	DBA
<input type="checkbox"/>	ORACLE	DELETE_CATALOG_ROLE
<input type="checkbox"/>	ORACLE	EXECUTE_CATALOG_ROLE
<input type="checkbox"/>	ORACLE	RECOVERY_CATALOG_OWNER
<input type="checkbox"/>	ORACLE	RESOURCE
<input type="checkbox"/>	ORACLE	SELECT_CATALOG_ROLE

Download

1-7

Add Row



Páginas de configuração de privilégios de sistema e a objetos

Home Configuration **Security Model** Report

Home > Configuration > System Privileges

System Privileges Cancel Delete Submit

<input type="checkbox"/>	Model Name	Privilege
<input type="checkbox"/>	ORACLE	ADMINISTER ANY SQL TUNING SET
<input type="checkbox"/>	ORACLE	ADMINISTER DATABASE TRIGGER
<input type="checkbox"/>	ORACLE	ADMINISTER RESOURCE MANAGER
<input type="checkbox"/>	ORACLE	ADMINISTER SQL MANAGEMENT OBJECT
<input type="checkbox"/>	ORACLE	ADMINISTER SQL TUNING SET
<input type="checkbox"/>	ORACLE	ADVISOR

Home Configuration **Security Model** Report

Home > Configuration > Object Privileges

Object Privileges Cancel Delete Submit

<input type="checkbox"/>	Model Name	Owner	Object Name	Privilege	Username
<input type="checkbox"/>	ORACLE	PERFSTAT	STATSSQLSUM	ALL	
<input type="checkbox"/>	ORACLE	PERFSTAT	STATSSQLTEXT	ALL	
<input type="checkbox"/>	ORACLE	SYS	ALL_SOURCE	ALL	
<input type="checkbox"/>	ORACLE	SYS	AUD\$	ALL	
<input type="checkbox"/>	ORACLE	SYS	DBA_%	ALL	

Página de configuração de parâmetros de instância

Home Configuration Security Model Report

Home > Configuration > Instance Parameters

Instance Parameters Cancel Delete Submit

Model Name	Name	Value	Description
ORACLE	<input type="text" value="_trace_files_public"/>	<input type="text" value="FALSE"/>	Prevents users from having the ability to read trace files which may contain sensitive information about the running Oracle instance.
ORACLE	<input type="text" value="audit_file_dest"/>	<input type="text" value="C:\APP\ORACLE\ADMIN\SEC\ADUMP"/>	The destination for the audit file must be set to a valid directory owned by oracle and set with owner read/write permissions only.
ORACLE	<input type="text" value="audit_sys_operations"/>	<input type="text" value="TRUE"/>	Auditing of the users authenticated as the SYSDBA or the SYSOPER provides an oversight of the most privileged of users.
ORACLE	<input type="text" value="audit_trail"/>	<input type="text" value="OS"/>	Ensures that basic audit features are used.
ORACLE	<input type="text" value="db_securefile"/>	<input type="text" value="ALWAYS"/>	Ensure that all LOB files created by Oracle are created as SecureFiles.
ORACLE	<input type="text" value="diagnostic_dest"/>	<input type="text" value="C:\APP\ORACLE"/>	The destination for the user dump must be set to a valid directory with permissions restricted to the owner of the Oracle software and the dba
ORACLE	<input type="text" value="global_names"/>	<input type="text" value="TRUE"/>	This parameter ensures that Oracle will check that the name of a database link is the same as that of the remote database.
ORACLE	<input type="text" value="o7_dictionary_accessibility"/>	<input type="text" value="FALSE"/>	This is a database initialization parameter that controls access to objects in the SYS schema.
ORACLE	<input type="text" value="os_authent_prefix"/>	<input type="text" value=""/>	OS roles are subject to control outside the database. The duties and responsibilities of DBAs and system administrators must be separated.
ORACLE	<input type="text" value="os_roles"/>	<input type="text" value="FALSE"/>	allows externally created groups to be used to manage database roles. This can lead to misaligned or inherited permissions.

Download

1-10 11:20 Add Row

Relatórios detalham os resultados da verificação do banco de dados

Home Configuration Security Model Report

Home > Database Parameters Report

Result

Select Timestamp: 09-OCT-2012 15.44.20.239000

Reports List

- Database Parameters
- Listener Parameters
- SQLNet Parameters
- Roles
- Object Privileges
- System Privileges
- Audit
- Profile
- Database
- Other Findings
- Conformity Chart

Go [Actions]








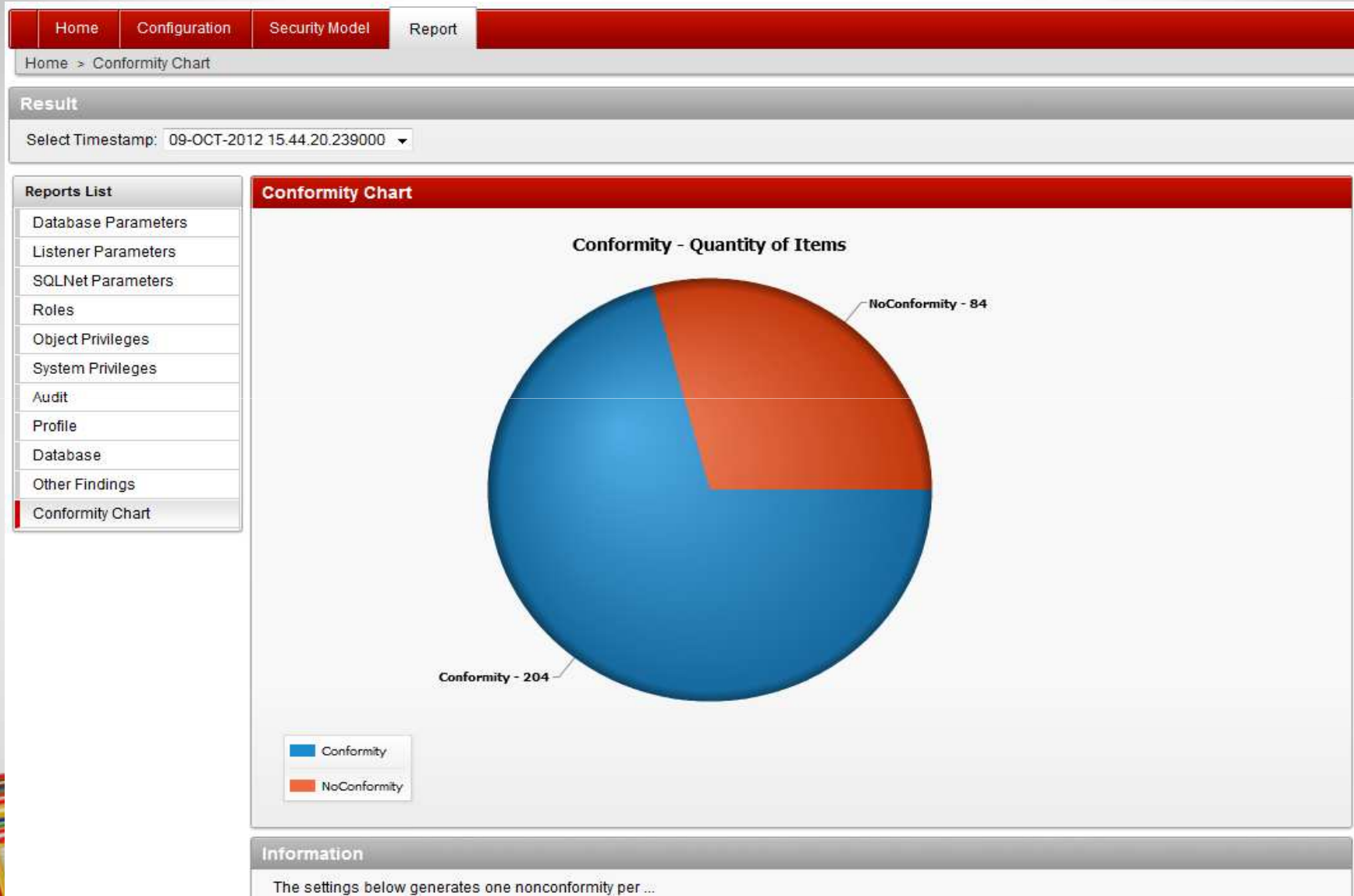
Parameter Name	Value	Expected Value	Message	Command
 global_names	FALSE	TRUE	This parameter ensures that Oracle will check that the name of a database link is the same as that of the remote database.	alter system set global_names=TRUE scope=both;
 audit_trail	NONE	OS	Ensures that basic audit features are used.	alter system set audit_trail=OS scope=both;
 sec_protocol_error_further_action	CONTINUE	DROP 60	When bad packets are received from a client the server will wait the specified number of seconds before allowing a connection from the same client. This help mitigate malicious connections or DOS conditions.	alter system set sec_protocol_error_further_action=DROP 60 scope=both;
 sec_protocol_error_trace_action	TRACE	ALERT	Specify the action a database should take when a bad packet is received.	alter system set sec_protocol_error_trace_action=ALERT scope=both;
 audit_sys_operations	FALSE	TRUE	Auditing of the users authenticated as the SYSDBA or the SYSOPER provides an oversight of the most privileged of users.	alter system set audit_sys_operations=TRUE scope=both;
 db_securefile	PERMITTED	ALWAYS	Ensure that all LOB files created by Oracle are created as SecureFiles.	alter system set db_securefile=ALWAYS scope=both;
 os_authent_prefix	OPSS	NULL	OS roles are subject to control outside the database. The duties and responsibilities of DBAs and system administrators must be separated.	alter system set os_authent_prefix="" scope=both;

Gráfico de conformidade



RESULTADOS E DISCUSSÕES

- Todos os objetivos foram atingidos;
- Profissionais que trabalham com banco de dados Oracle efetuaram os testes no sistema.



CONCLUSÃO

- Empresas e pessoas estão dando cada vez mais importância a segurança da informação;
- Preocupação em garantir a confidencialidade das informações armazenadas;
- Sistema atende as necessidades e acelera o processo de auditoria, diminuindo a possibilidade de ocorrência de erros.



EXTENSÕES

- Avaliar a segurança do sistema operacional;
- Bancos de dados como itens de configuração;
- Níveis de configuração;
- Níveis de pontuação.



REFERÊNCIAS

BRYLA, Bob; LONEY, Kevin. Oracle database 11g manual do dba. Tradução Altair Caldas Dias de Moraes. Porto Alegre: Bookman, 2009.

KYTE, Thomas. Expert Oracle database architecture, 2nd edition. New York, NY: Apress, 2010.

LONEY, Kevin. Oracle database 11g the complete reference. New York, NY: McGraw-Hill, 2009.

NATAN, Ron Ben. HOWTO secure and audit Oracle 10g and 11g. Boca Raton, FL: CRC Press, 2009.

NATAN, Ron Ben. Implementing database security and auditing. Burlington, MA: Elsevier, 2005.

STEWART, James Michael; TITTEL Ed; CHAPPLE Mike. CISSP: certified information systems security professional study guide 3rd edition. Alameda, CA: Sybex, 2005.

WALLACE, Kathryn. Common criteria and protection profiles: how to evaluate information technology security. [Bethesda, MD], 2003. Disponível em: <http://www.sans.org/reading_room/whitepapers/standards/common-criteria-protection-profiles-evaluate-information_1078>. Acesso em: 16 out. 2012.

WATSON, John; RAMKLASS, Roopesh; BRYLA, Bob. OCA/OCP Oracle database 11g all-in-one exam guide. New York, NY: McGraw-Hill, 2010.

WATSON, John. OCA Oracle database 11g administração I. Tradução Altair Caldas Dias de Moraes. Porto Alegre: Bookman, 2010.





DEMONSTRAÇÃO DO SISTEMA

