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).

Commom Criteria

O *Commom 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 principio 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

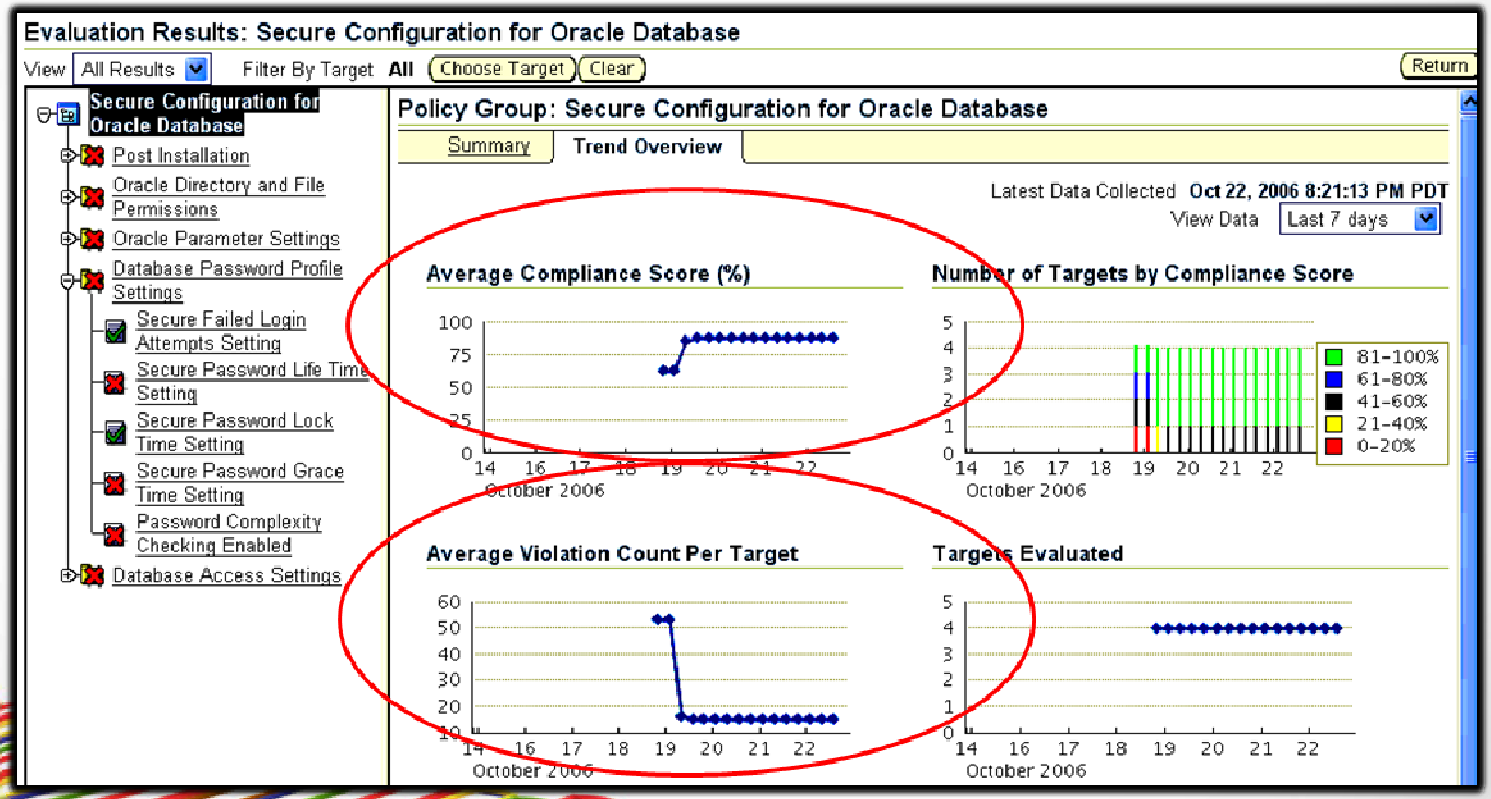
A necessidade de verificar as configurações relacionadas à segurança é uma demanda anual de um cliente da Teclógica.

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 politicas 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.

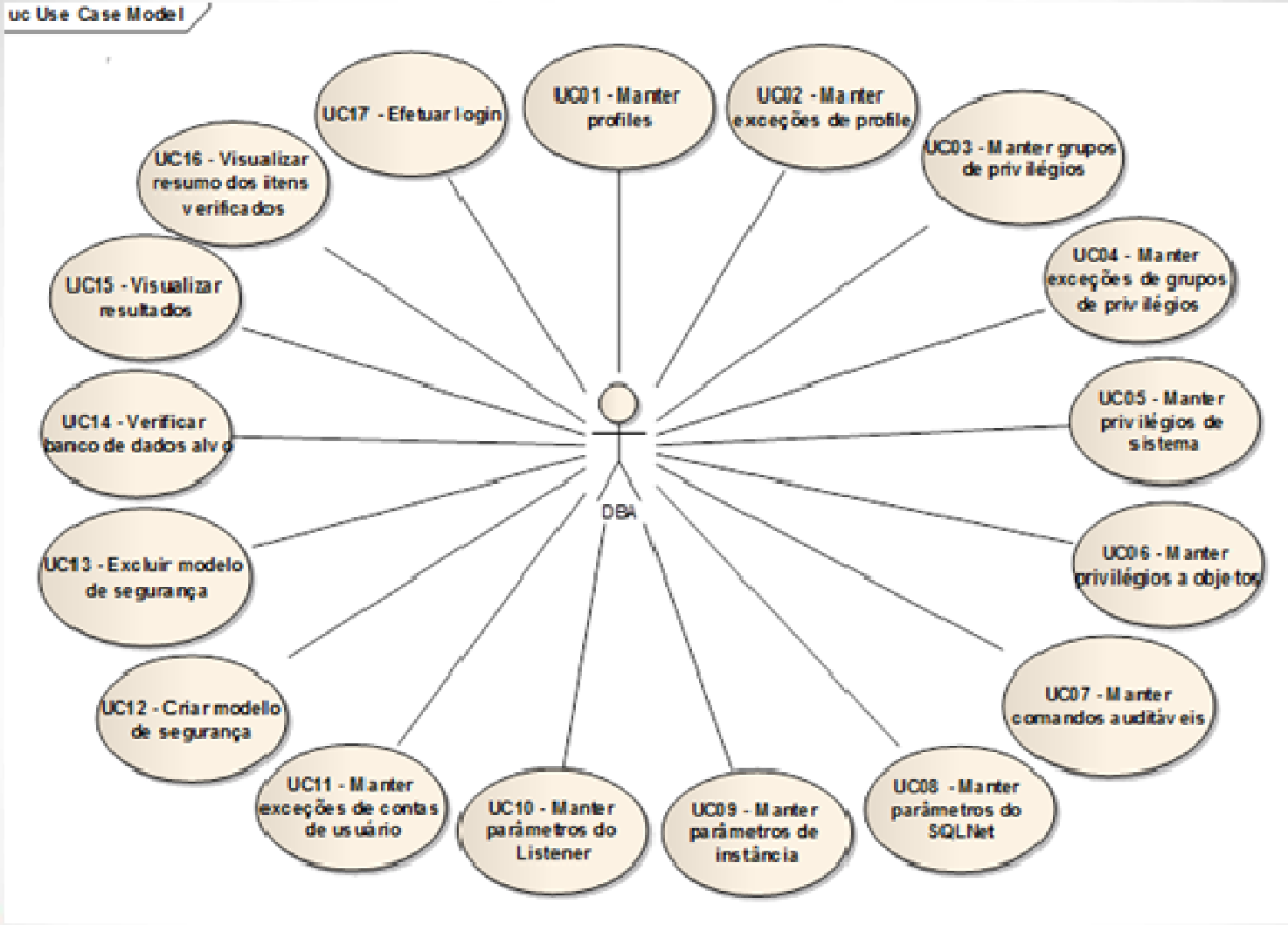
Visualizar:

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

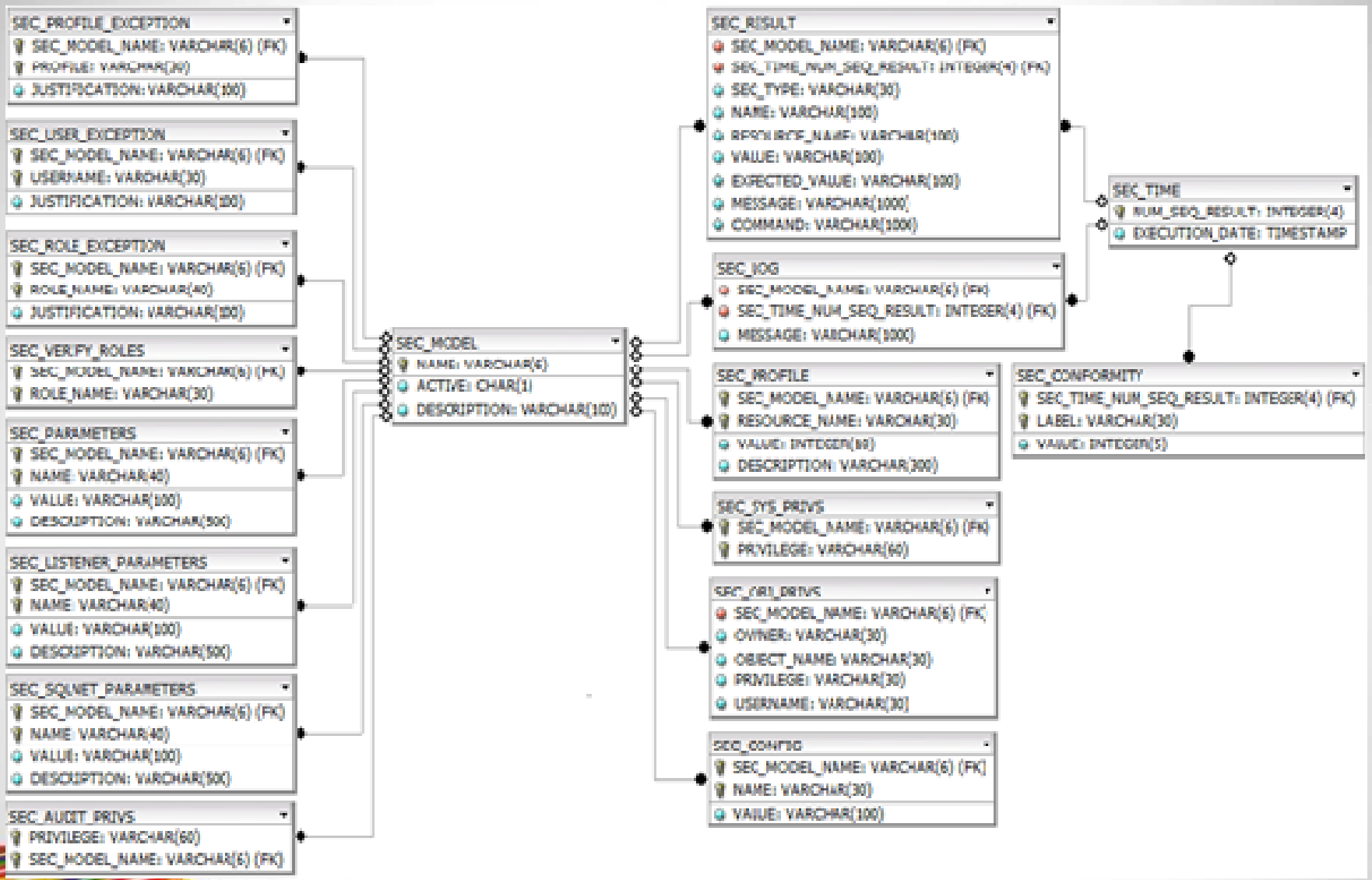
Requisitos Não Funcionais

- 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:

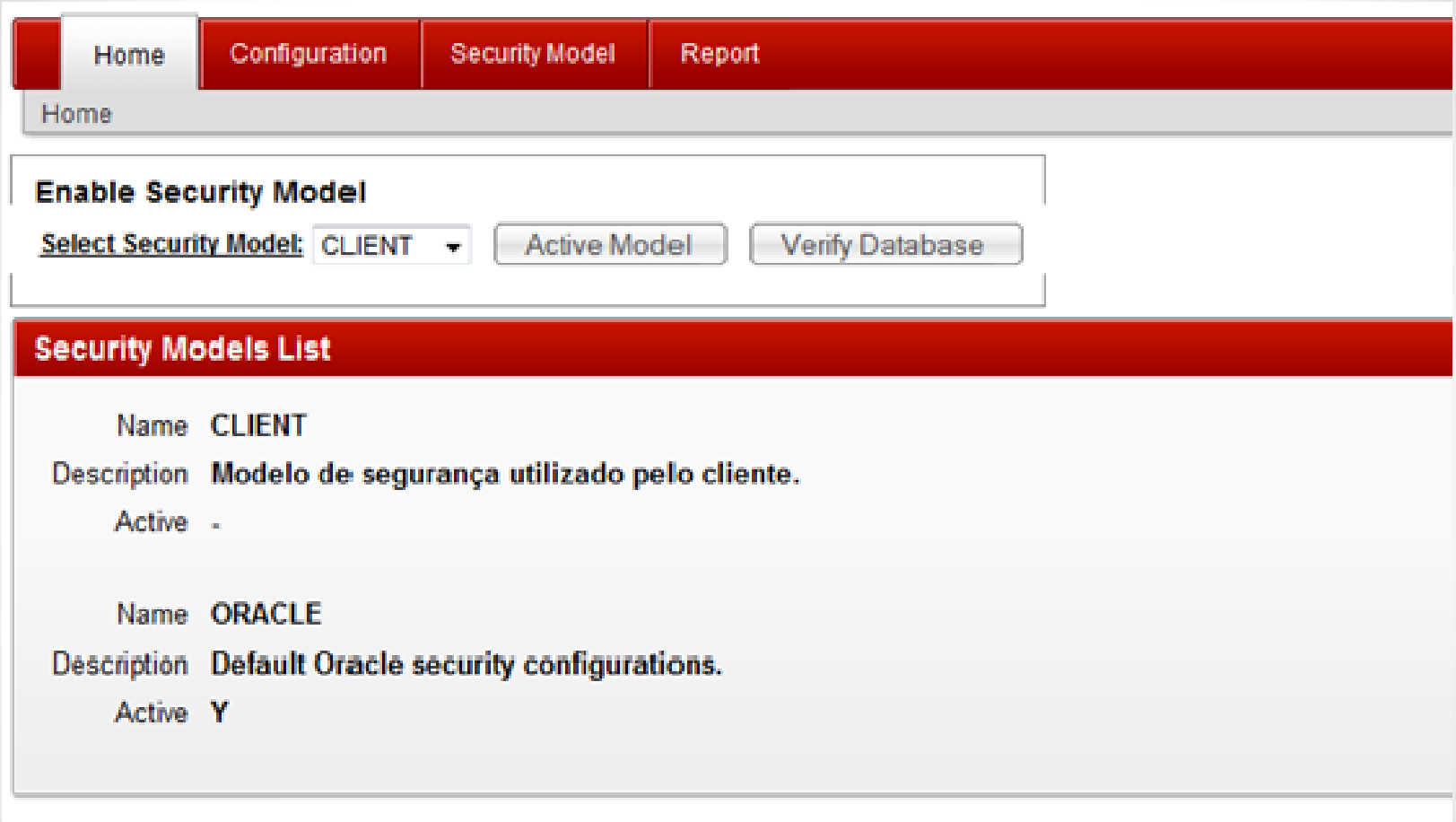
- SQL Developer;
- Application Builder (Oracle Application Express).

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

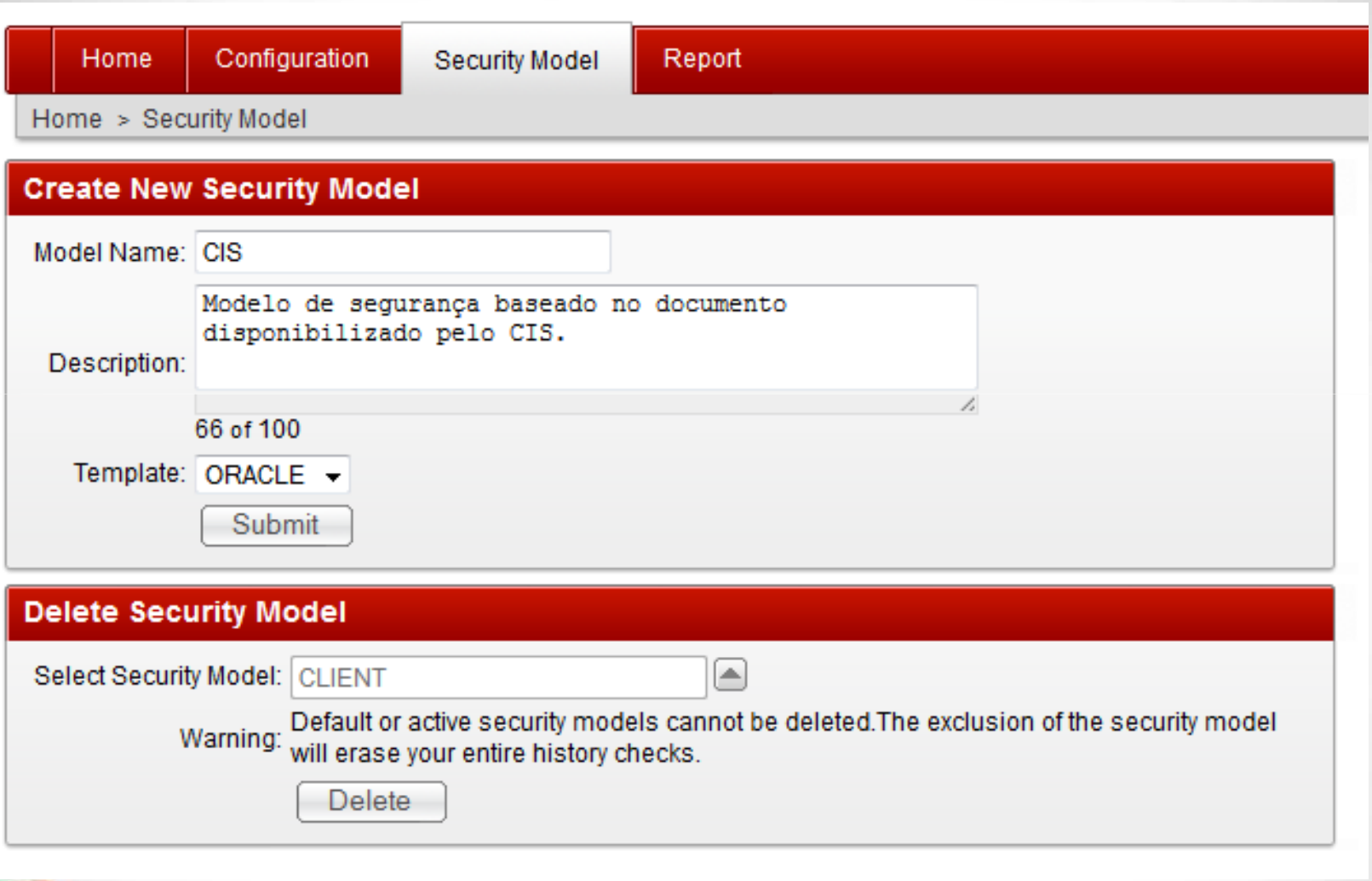
Servidor *web*: Oracle Weblogic 11g.

OPERACIONALIDADE DA IMPLEMENTAÇÃO

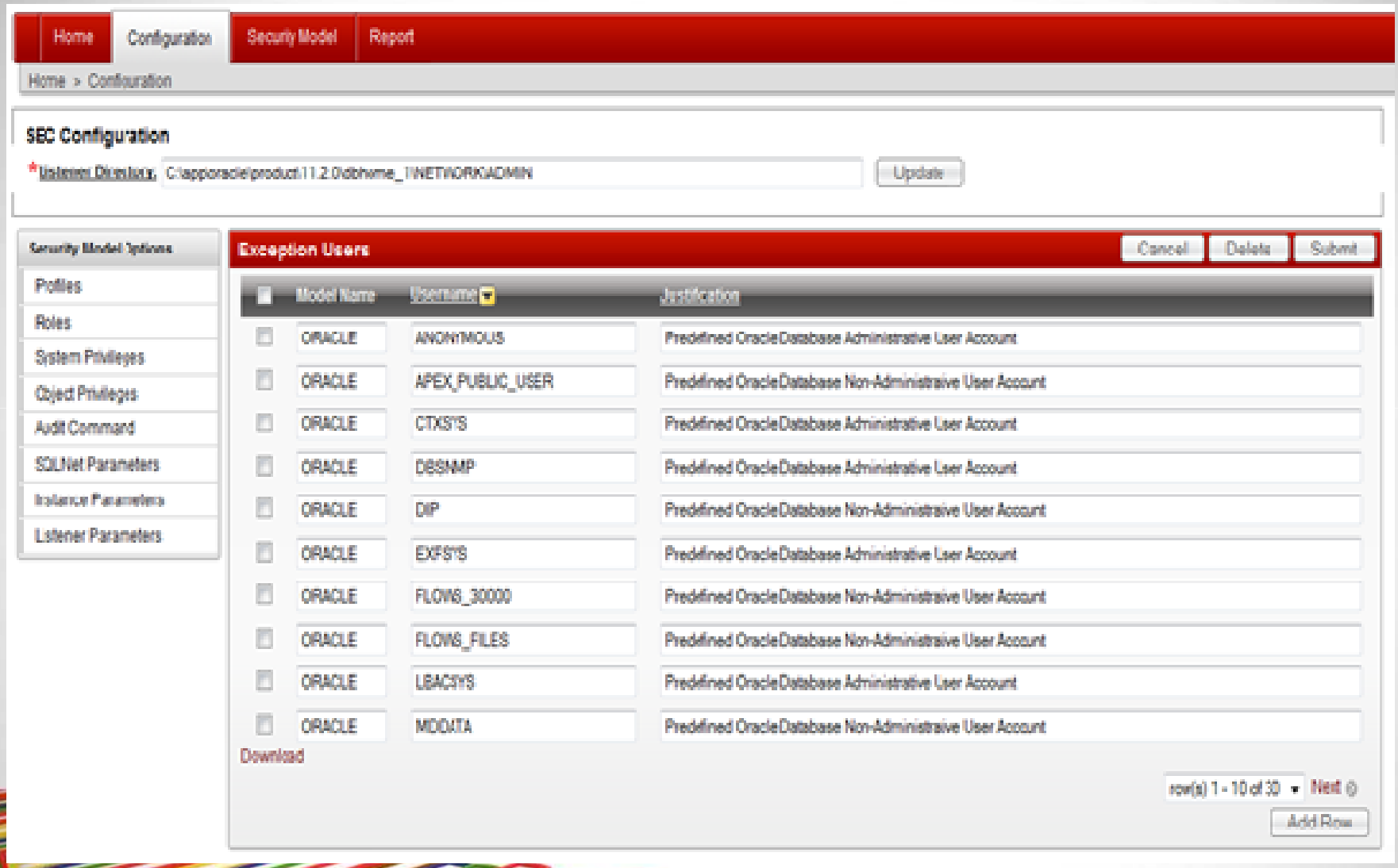
Página inicial do sistema



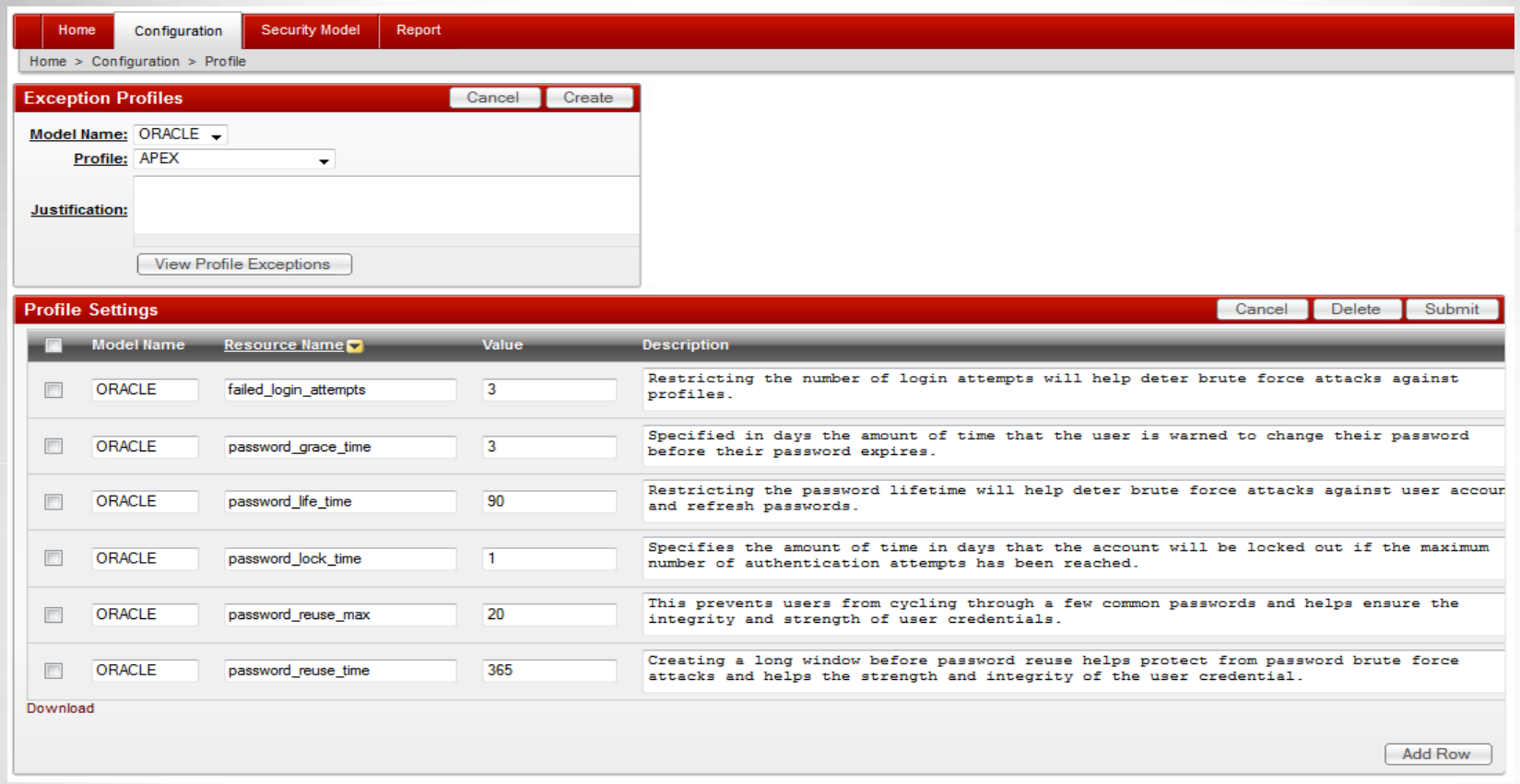
Página de criação e exclusão de modelo de segurança



Página principal de configuração

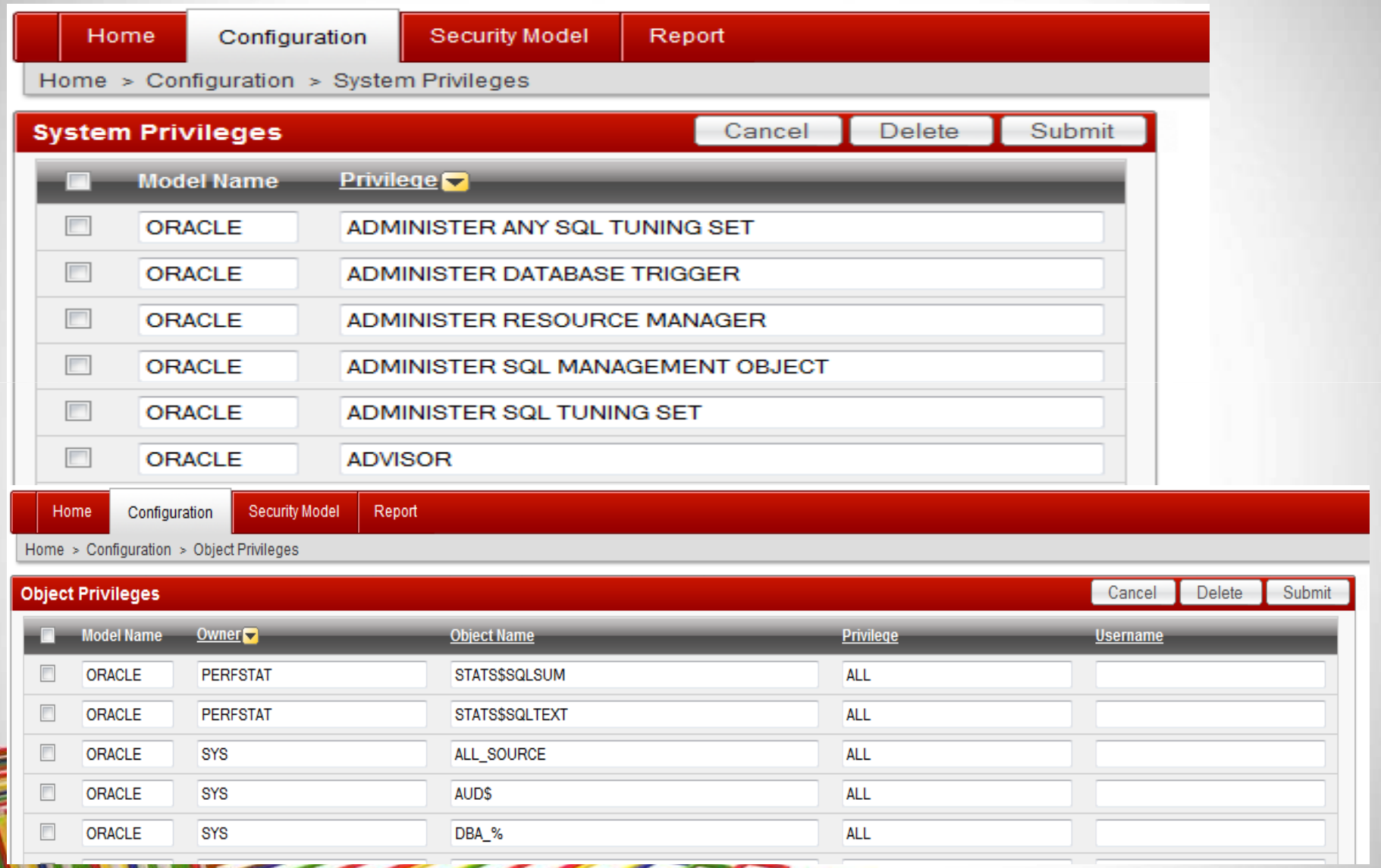


Página de configuração de *profiles* de conta de usuário

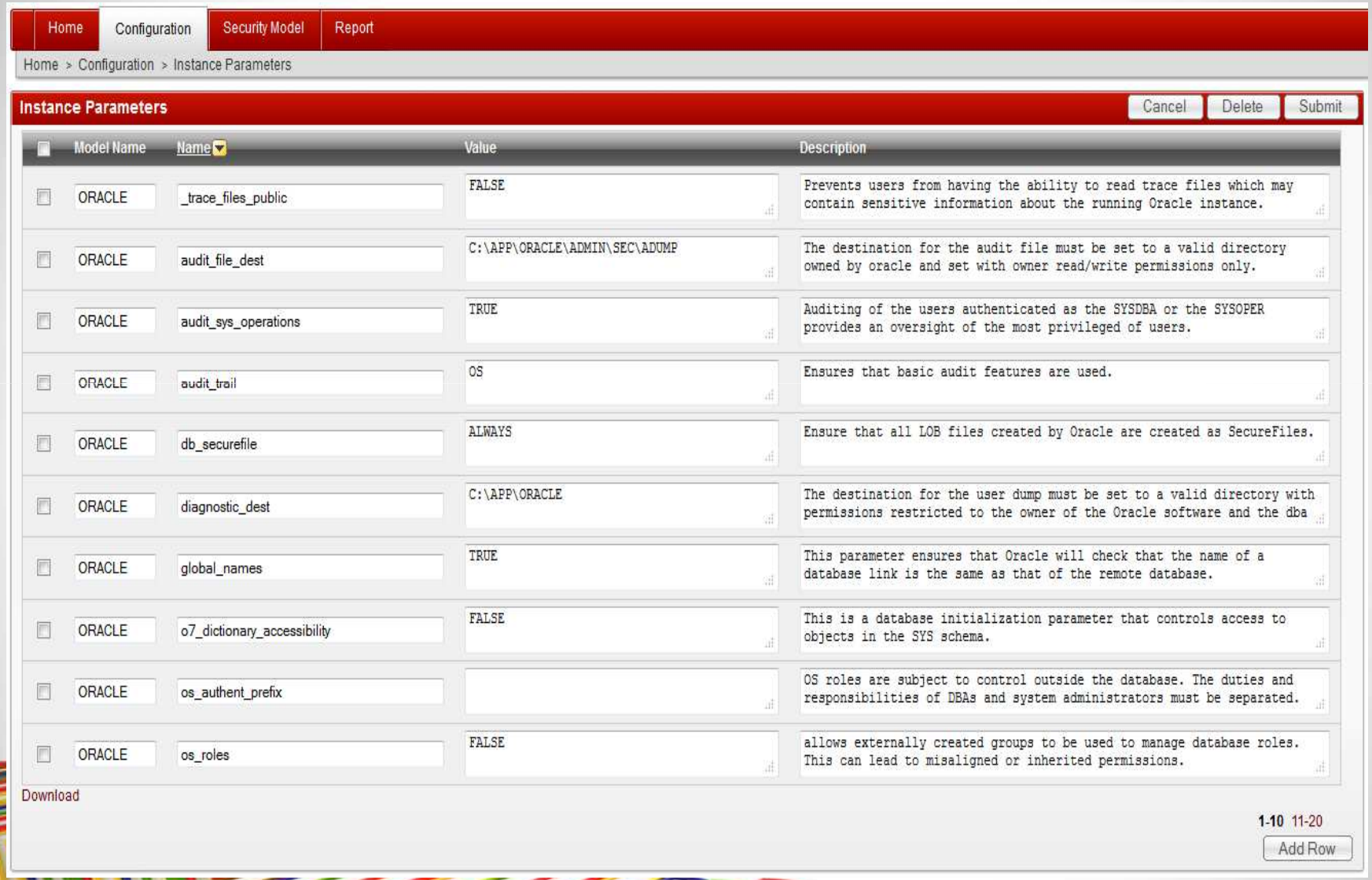


Página de configurações de *roles*

Páginas de configuração de privilégios de sistema e a objetos



Página de configuração de parâmetros de instância



Relatórios detalham os resultados da verificação do banco de dados

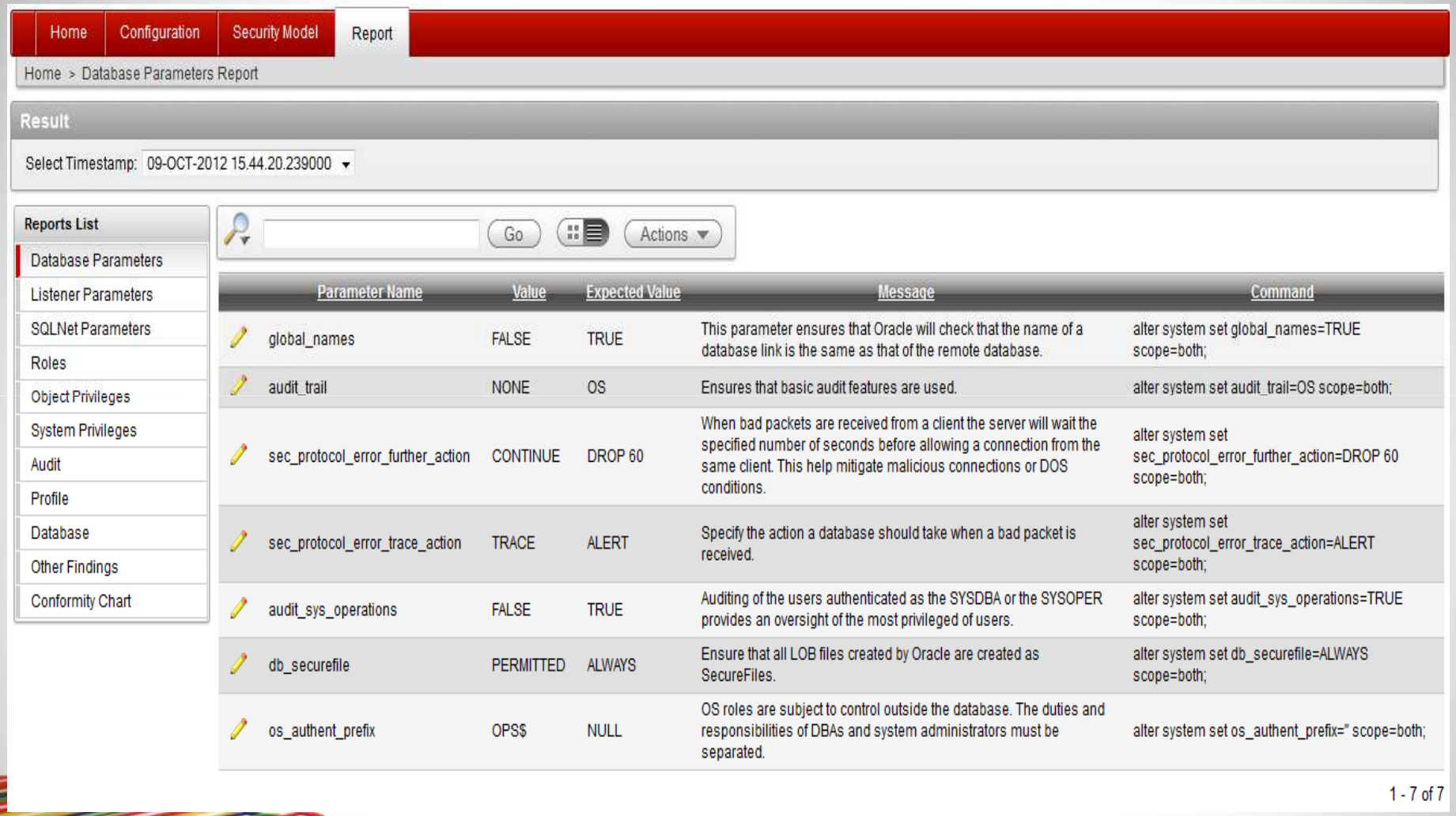
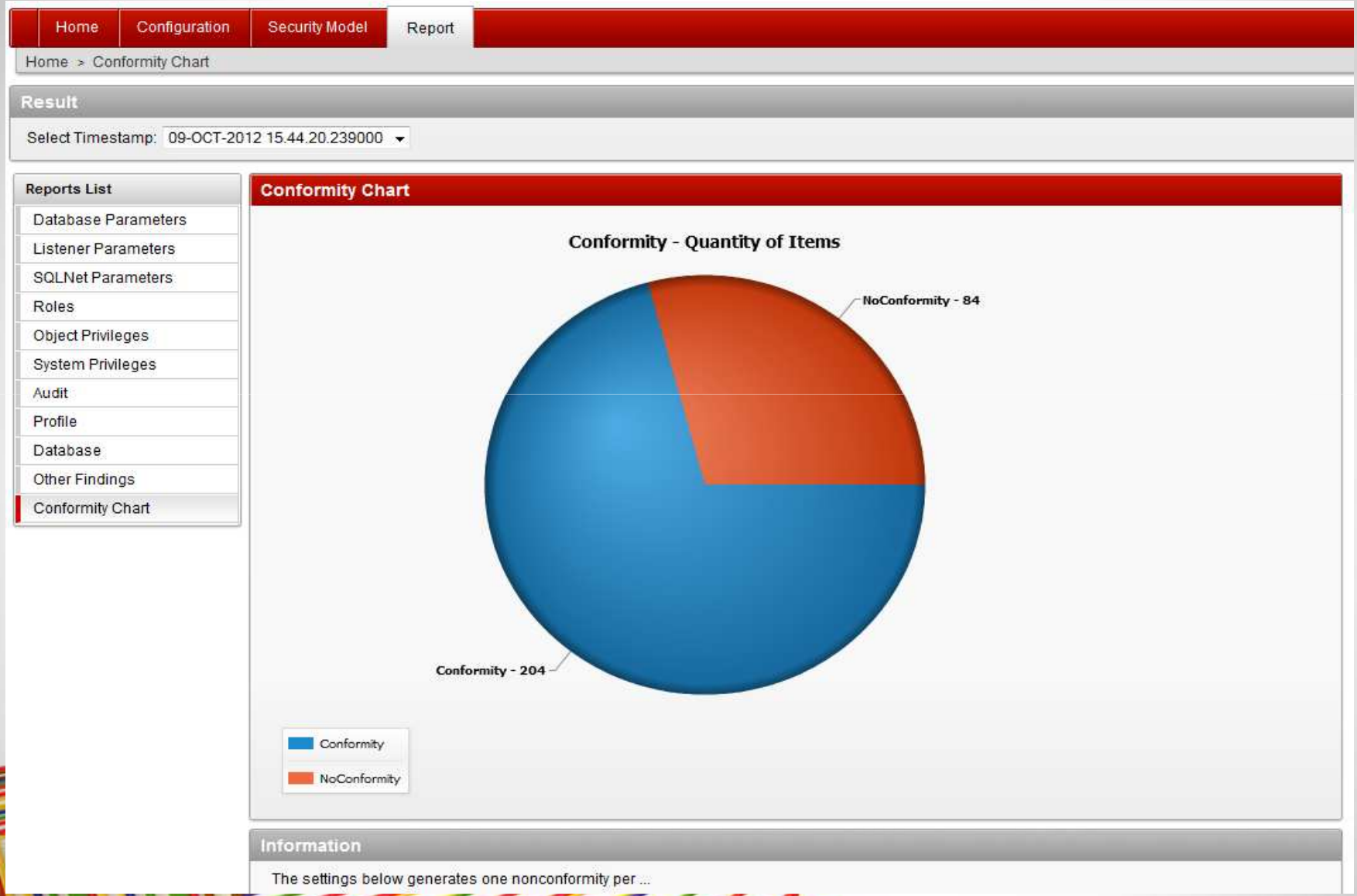
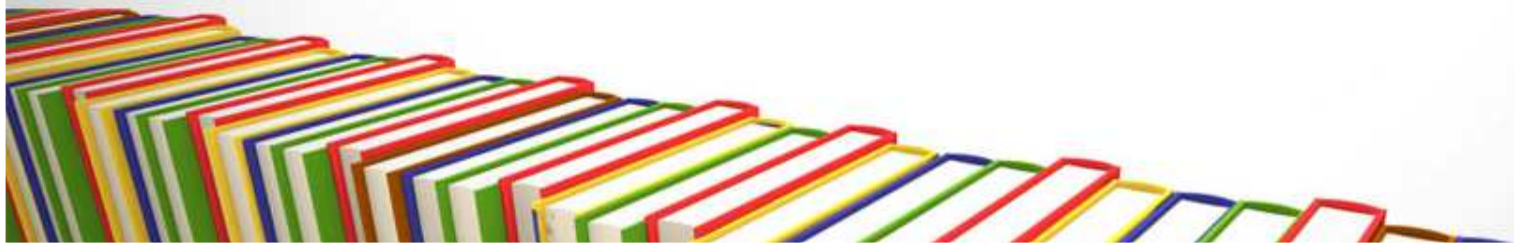


Gráfico de conformidade



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