CENTRO PAULA SOUZA

FACULDADE DE TECNOLOGIA DE AMERICANA

Curso Segurança da informação

César Augusto Florian

ALTA DISPONIBILIDADE EM BANCO DE DADOS

Americana, SP

2015

CENTRO PAULA SOUZA

FACULDADE DE TECNOLOGIA DE AMERICANA

Curso Segurança da informação

César Augusto Florian

ALTA DISPONIBILIDADE EM BANCO DE DADOS

Trabalho de Conclusão de Curso desenvolvido em cumprimento à exigência curricular do Curso Segurança da Informação, sob a orientação do Prof. Esp. Edson Roberto Gaseta

Área de concentração: Segurança da Informação

Americana, S. P.

2015

Florian, César Augusto
F659a Alta disponibilidade em banco de dados. / César Augusto Florian. – Americana: 2015.
39f.

Monografia (Graduação em Tecnologia em Segurança da Informação). - - Faculdade de Tecnologia de Americana – Centro Estadual de Educação Tecnológica Paula Souza.
Orientador: Prof. Esp. Edson Roberto Gaseta

1. Banco de dados I. Gaseta, Edson Roberto II. Centro Estadual de Educação Tecnológica Paula Souza – Faculdade de Tecnologia de Americana.

CDU:681.3.07

César Augusto Florian

Alta disponibilidade de banco de dados

Trabalho de graduação apresentado como exigência parcial para obtenção do título de Tecnólogo em Segurança da informação pelo CEETEPS/Faculdade de Tecnologia – Fatec/ Americana.
Área de concentração: Segurança da Informação

Americana, 11 de dezembro de 2015.

Banca Examinadora:

Edson Roberto Gaseta (Presidente)
Especialista
Fatec Americana

Juliane Borsato Beckedorff Pinto (Membro)
Tecnólogo
Fatec Americana

Rodrigo Brito Battilana (Membro)
Bacharel
Fatec Americana

AGRADECIMENTOS

Em primeiro lugar a Deus por me ajudar nos momentos de dificuldades. À minha familia e minha noiva Michele Godoy que me apoiaram durante todo o período de graduação. Ao meu orientador Edson Roberto Gaseta, pelo suporte durante a produção deste trabalho. E por fim a todos que direta ou indiretamente fizeram parte da minha formação.

DEDICATÓRIA

Aos meus pais, amigos, companheiros de trabalho e minha noiva Michele Godoy.

RESUMO

A presente monografia aborda aspectos sobre a importância da tecnologia da informação e do profissional que atua nesta área, conceitua o que é segurança da informação e foca em um dos seus principais pilares, a disponibilidade. São abordados conceitos relevantes para o assunto como SLA, tipos de parada de serviço, redundância, *clusters* e classificações de disponibilidade. O texto tem como principal objeto de estudo ferramentas usadas em alta disponibilidade de banco de dados, especificamente Oracle Real Application Cluster (RAC). São citados seus principais componentes, uma breve explanação de seu funcionamento e um estudo de caso demonstrando o failover de sessões durante a execução de atividades no banco de dados. A monografia não aborda aspectos da instalação do RAC, apenas demonstra seu funcionamento.O objetivo do trabalho é destacar a importância da alta disponibilidade e mostrar uma alternativa com potencial para alcança-la no que se refere a acesso a banco de dados. O método utilizado é a demonstração prática da solução em um ambiente virtualizado. A conclusão é de que o Oracle Real Application tem potencial de manter o acesso ao banco de dados 100% do tempo disponível para a aplicação.

Palavras Chave: Segurança da informação; disponibilidade; banco de dados

ABSTRACT

This monograph deals with aspects about the importance of information technology and the professionals who work in this area, it defines what is information security and focuses on one of its main pillars, availability. Relevant concepts to the theme are covered such as SLA, types of service failures, redundancy, clustering and the classification of availability. The text's main objects of study are tools used in high availability for databases, specifically Oracle Real application cluster (RAC). It cites RAC main components, a brief explanation of their operation and a study case demonstrating the failover sessions during the execution of activities in the database.
The monograph does not address aspects of the RAC installation, only demonstrates its operation.
The objective is to highlight the importance of high availability and show an alternative with the potential to reach it regarding access to databases.
The method used was practical demonstration of the solution in a virtualized environment.
The conclusion is that Oracle Real Application has the potential to maintain access to the database 100% of the time available for application.

Keywords: *Information security; availability; database.*

SUMÁRIO

LISTA DE FIGURAS

LISTA DE ABREVIATURAS E SIGLAS

NAS	Network Access Storage
RAC	Real Application Cluster
RAID	Redundant Array of Independent Discs
SAN	Storage Area Network
SGBDR	Sistema Gerenciador de Banco de Dados Relacional
SLA	Service Level Agreement
SQL	Structured Query Language
TI	Tecnologia da Informação
VIP	Virtual Internet Protocol

1 INTRODUÇÃO

O presente trabalho foi desenvolvido com o objetivo de conceituar o que é segurança da informação e destacar a importância da TI e do profissional de segurança desta área.

Como objetivos específicos esta monografia pretende apresentar as soluções existentes para alta disponibilidade em banco de dados e mostrar uma solução que apresenta potencial de manter a disponibilidade do banco de dados.

O método científico de pesquisa utilizado foi a consulta de autores que escreveram sobre o assunto de segurança da informação em livros, artigos, monografias e documentos técnicos.

O trabalho foi estruturado em oito capítulos, sendo o primeiro a própria introdução, o segundo apresenta a importância da TI e do profissional de segurança em TI, o terceiro conceitua o que é segurança da informação, o quarto se concentra em disponibilidade, um dos principais pilares da segurança da informação, o quinto apresenta as soluções mais utilizadas para alta disponibilidade em banco de dados, o sexto dá profundidade na solução conhecida como *Oracle Real Application Cluster* e o sétimo mostra um estudo de caso utilizando máquinas virtuais.

Com base nas informações conseguidas a partir dos estudos realizados nos capítulos anteriores, o capítulo oitavo se reserva às considerações finais.

2 A IMPORTÂNCIA DA TECNOLOGIA DA INFORMAÇÃO (TI) E DO PROFISSIONAL DE SEGURANÇA DA INFORMAÇÃO

Refere-se a TI, o departamento responsável por cuidar da tecnologia da informação de uma empresa ou entidade pública ou privada.

Para Marques (2014) a tecnologia da informação é parte da rotina das organizações, seja contribuindo com a sua eficiência na gestão das informações, no apoio a decisões gerando diferencial competitivo ou afetando interesses e valores centrados em pessoas.

Ainda segundo Marques (2014):

> "A velocidade com que a informação e o conhecimento são criados e circulam sem fronteiras, potencializa a importância do capital intelectual. As organizações dotadas de Inteligência Empresarial, estrategicamente apoiada pela Tecnologia da Informação (TI), certamente estarão à frente no mundo dos negócios".

É cada vez mais comum observar a transformação da TI que antes era um departamento que gerava custos, e agora é cada vez mais vista como um investimento apoiando as operações de negócio e trazendo retorno. Com o auxílio da TI, processos operacionais, antes executados de maneira manual, podem ser simplificados ou automatizados, trazendo agilidade para as operações. Além disso, as informações geradas e processadas rapidamente ajudam na tomada de decisão, trazendo grande vantagem para a empresa tanto no seu setor estratégico como operacional.

De acordo com Taurion (2013) da maneira que a TI está cada vez mais relacionada ao negócio, existe a possibilidade da TI deixar de fazer parte do negócio e se tornar o próprio negócio no futuro. Também segundo ele, as empresas que não estão com o departamento de TI alinhados com sua estratégia, estão perdendo competitividade e precisam se adequar o quanto antes para sobreviverem.

Com o crescente número de investimento na área da TI, é esperado também que cada vez mais as empresas busquem alternativas para manter sua tecnologia segura. É coerente manter esforços e investimento com o objetivo de proteger um elemento tão preciso ao negócio. Para auxiliar em tal função, existem os especialistas em segurança da informação. De acordo com Daquino (2010) este

profissional deve utilizar de seus conhecimentos para ajudar a prevenir que as informações sigilosas sejam roubadas ou vazadas a concorrentes por exemplo.

Segundo Silva Junior (2010) o profissional de segurança tem a missão de assegurar disponibilidade das informações, resguardar a integridade de tais informações e também garantir confidencialidade em relação a seu conteúdo.

Ainda em relação aos profissionais de TI, Daquino (2010) cita que a profissão de especialista em segurança da informação não é amplamente conhecida por boa parte da população, mas que isso não diminui a importância que esses profissionais têm para a sociedade. Como é uma profissão relativamente nova, já que nasceu e vem crescendo junto com a era da tecnologia moderna, a quantidade de profissionais atuando nesta área e o número de profissionais neste ramo de atividade no mercado ainda é baixo se comparado com as demais profissões mais antigas. Porém é tendência que esses profissionais sejam cada vez mais requisitados.

No próximo capítulo será abordado a definição de segurança da informação e seus aspectos

3 SEGURANÇA DA INFORMAÇÃO

Segundo Fontes (2008, p. 6) "A informação sempre foi um dos bens mais importantes da organização.". Não é difícil imaginar que uma empresa sem a documentação de suas principais atividades, sem troca de informações entre departamentos, sem dados históricos sobre suas operações ou mesmo sem a sua lista de fornecedores seria incapaz de operar independentemente da sua área de atuação. Atualmente informação está em todos os segmentos e departamentos de um negócio. Fontes (2008, p. 7) "Encare a segurança da informação como um elemento crítico que possibilita a realização do negócio".

Segundo Loureiro (2008, p. 15) a norma ABNT NBR ISO/IEC 27002 define:

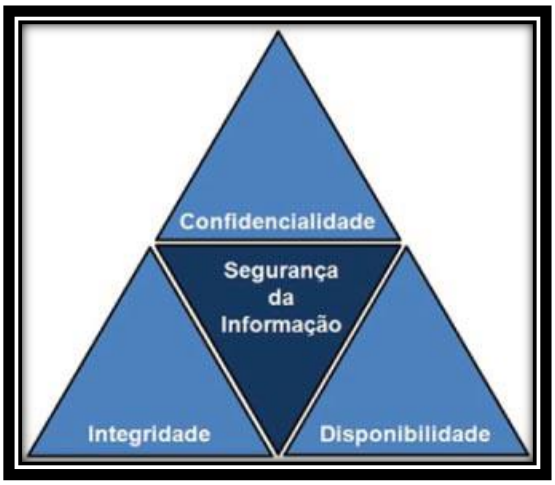
> “Segurança da informação é a proteção da informação de vários tipos de ameaças para garantir a continuidade do negócio, minimizar o risco ao negócio, maximizar o retorno sobre os investimentos e as oportunidades de negócio.”

Ao longo dos anos, a informação que antes era mantida em meios não digitais foi aos poucos substituída, sendo manipuladas e armazenadas hoje por meios mais tecnológicos, como computadores, celulares, mídias de armazenamento digitais, e mais recentemente em recursos na rede chamados de nuvem. Essa mudança se deve principalmente à agilidade que os meios digitais proporcionam ao lidar com essas informações. Hoje os recursos tecnológicos que lidam com as informações tem um papel chave na tomada de decisão das empresas e por esta razão a agilidade é fundamental. Além da agilidade é preciso que as informações permaneçam seguras, visto que muitas vezes elas carregam informações confidencias sobre usuários, ou mesmo informações estratégicas da companhia.

A segurança da informação tem aqui um papel fundamental. De acordo com Fontes (2008, p. 8) "[...] existe para possibilitar que o negócio da organização aconteça de forma protegida no que diz respeito aos recursos de informação."

Para garantir que a informação esteja segura, existem 3 pilares chaves que devem ser garantidos, conhecidos como tríade da segurança, e são eles confidencialidade, integridade e disponibilidade.

Figura 1 – Tríade da segurança da informação



Fonte: Macêdo (2012)

Em síntese, a seguir estão apresentados cada um dos pilares:

Confidencialidade: A informação deve estar disponível somente para aqueles que precisam ter acesso a ela. Independentemente do nível hierárquico de um indivíduo dentro da companhia, ele só terá acesso às informações que são necessárias para desempenhar o seu papel dentro do processo ou atividade corporativa. É importante também garantir mecanismos para que terceiros não consigam roubar, ou se beneficiar das informações confidenciais em nenhum momento do processo, seja ele no seu armazenamento ou na sua transmissão.

Integridade: É preciso garantir que as informações que são armazenadas, transmitidas e manipuladas sejam verdadeiras e fiéis a realidade. Elas não podem ser corrompidas, destruídas ou manipuladas por terceiros não autorizados de forma alguma. Isso inviabilizaria a utilização de tais informações e em muitos casos, se não fossem notados os problemas de integridade, levariam a tomadas de decisões erradas dentre outros problemas.

Disponibilidade: A informação deve estar acessível para que seja utilizada sempre que necessário dentro de um processo. Uma informação indisponível faz com que um processo ou serviço fique parado causando prejuízo e inoperabilidade dentro da companhia. Ela pode ainda impedir a tomada de decisão durante a sua

indisponibilidade. Quanto maior for a criticidade da informação, maior será o prejuízo de sua indisponibilidade e maior deve ser o esforço para garantir sua disponibilidade.

No capítulo seguinte, será dado mais profundidade à disponibilidade, um dos pilares fundamentais da segurança da informação.

4 DISPONIBILIDADE

Segundo Fontes (2008, p. 166) um dos objetivos da segurança da informação é a disponibilidade dessa informação para a realização do negócio.

Desde sempre a informação tem papel chave nas operações da sociedade. Isso, evidentemente engloba as empresas e instituições públicas e até mesmo o dia a dia das pessoas. Com a atual tecnologia, a informação está diariamente trafegando entre essas instituições e usuários para a realização de diversas atividades da sociedade, como efetuar pagamentos, contratar serviços e durante a produção de manufatura. Para a execução de tais tarefas, tornou-se imprescindível a utilização de sistemas tecnológicos que empregam agilidade, rapidez e muitas vezes possibilitam a automatização dessas tarefas. Estes sistemas deixaram de ser um diferencial e se tornaram indispensáveis para a existência de diversos tipos de negócios. Hoje é impossível imaginar uma empresa que não empregue tal infraestrutura em seu funcionamento e continue a ser competitiva no mercado.

Os sistemas de informação estão tão ligados ao negócio que a parada de um sistema na maioria das vezes significa a parada de processos e serviços essenciais de uma companhia.

4.1 Tipos de parada de serviços

Podem-se ter basicamente dois tipos de paradas de serviço:

- Paradas planejadas: são aquelas onde existe um planejamento prévio de parar determinado sistema de informação para a realização de manutenções, troca de equipamentos ou *upgrade* de determinados sistemas.
- Paradas não planejadas: são aquelas onde o sistema para de funcionar, em um momento que era esperado que o mesmo estivesse funcionado. Este segundo caso, muito mais crítico, uma vez que indisponibiliza o uso de dado sistema em tempo de operação.

Além do prejuízo que uma parada não planejada pode causar nas operações de uma empresa, o mesmo pode afetar a imagem de uma instituição se o serviço em questão afetar terceiros, como por exemplo uma empresa de cartão de crédito que por alguma falha em seu sistema impede que usuários efetuem a compra em

diversos outros estabelecimentos. Aqui em adição do prejuízo que a empresa deve sofrer com multas por não conseguir prestar o serviço acordado, ela também vai sofrer com o impacto negativo que isso terá em sua imagem perante o público e demais empresas do setor, já que estas podem optar por evitar escolher tal prestadora de serviço no futuro.

4.2 SLA (Service Level Agreement)

Com o objetivo de proteger as partes contratantes e contratadas em prestação de serviços, existe o SLA (Service Level Agreement). De acordo com Canalonga (2014) o SLA é um acordo previamente estabelecido entre as partes que prevê de maneira mensurável os requisitos de entrega de um serviço tanto em quantidade como em qualidade. Exemplo disso seria o acordo entre uma companhia de internet e uma empresa onde a mesma estabelece que precise de no mínimo 90% de tempo de disponibilidade de sua rede ao longo de determinado período. Em caso de não cumprimento dos termos acordados a empresa contratante recebe da empresa contratada uma multa. Em contrapartida, a empresa que presta o serviço cobra o valor baseado nos requisitos do SLA, e tem que se planejar para entregar o mínimo acordado em contrato.

Existem hoje grandes prestadoras de serviço que atuam em sistemas críticos que tem SLA de 100% de tempo de disponibilidade ou muito próximos a isto. Estas empresas precisam adotar técnicas de redundância para garantir que o sistema fique disponível mesmo com a eventual falha em um dos seus equipamentos.

4.3 Redundâncias e *clusters*

Pode-se citar dentre as técnicas de alta disponibilidade mais amplamente implementadas em servidores que necessitam de disponibilidade:

Cluster de servidores: onde temos mais de um servidor atuando em conjunto para a realização de determinada tarefa. No caso de falha de um dos equipamentos os outros conseguem continuar com a carga de trabalho. Cada conjunto de equipamentos com capacidade para executar a tarefa dentro do *cluster* é chamado de nó. O conjunto de vários nós compõem o *cluster*.

Sanchez (2013) afirma que *Storage* que em português brasileiro pode ser traduzido como armazenamento, e trata-se do conjunto de dispositivos geralmente de alta desempenho dedicados a armazenar dados.

Em um ambiente com alta disponibilidade geralmente são utilizados *storages* compartilhados e com diferentes níveis de redundância e recuperação de falhas, os chamados RAIDs. De acordo com Brito (2012) :

> "RAID (*Redundant Array of Independent Disks* ou Conjunto Redundante de Discos Independentes) é uma tecnologia utilizada principalmente em servidores que consiste em um conjunto de dois ou mais discos rígidos. Ela possui dois objetivos básicos: tornar o sistema de disco mais rápido, com o uso de Divisão de dados (RAID 0); ou tornar o sistema de disco mais seguro, usando a técnica de Espelhamento (RAID 1). As duas técnicas podem ser usadas isoladamente ou em conjunto."

Este trabalho não tem o objetivo de explicar RAID em detalhes, apenas de citar sua utilização.

Pode-se ainda contar com links de internet redundantes e mesmo redundância de rede local.

Todas essas redundâncias servem para evitar ao máximo que sistemas críticos e com alta demanda de disponibilidade acordados em SLA fiquem o máximo de tempo disponíveis, chegando próximos a 100% de disponibilidade.

Segundo Pereira (2005) existem três tipos de disponibilidade:

- Básica: Disponibilidade em que o sistema possui componentes suficientes para manter seu funcionamento. No caso de falha de um dos componentes haverá uma indisponibilidade no sistema percebida pelo usuário.
- Alta Disponibilidade: Disponibilidade que conta com redundância nos componentes. No caso de falha a mesma é mascarada por outro componente redundante sendo transparente para o usuário.
- Disponibilidade Contínua: Disponibilidade onde os componentes ficam 100% do tempo disponíveis, mesmo em paradas não planejadas, a disponibilidade é mantida.

A alta disponibilidade e a disponibilidade contínua asseguram que uma falha de um componente não afetara o serviço prestado ao usuário.

Um dos elementos que compõem praticamente todas as aplicações atuais é o banco de dados e sua infraestrutura. De nada adiantaria implementar toda uma redundância e com *clusters* no ambiente se o próprio banco de dados de uma aplicação ficar indisponível. Pensando nisso, os principais fornecedores de banco de dados do mercado desenvolveram técnicas de alta disponibilidade também para o banco de dados e seu sistema gerenciador.

No capítulo seguinte serão mostradas as opções existentes no mercado para alta disponibilidade de banco de dados.

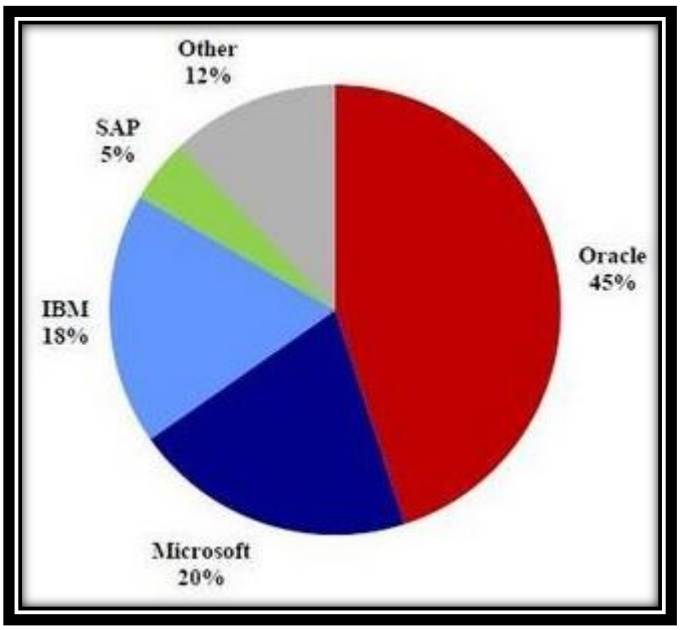
5 FERRAMENTAS PARA ALTA DISPONIBILIDADE EM SGBDR

Por definição, de acordo com Dias Neto (2015):

> “Sistema Gerenciador de Banco de Dados Relacional (SGBDR) é um software que controla o armazenamento, recuperação, exclusão, segurança e integridade dos dados em um banco de dados.”

Segundo pesquisa divulgada por Shukla (2014), Oracle, IBM e Microsoft aparecem como os principais provedores de SGBDR no mundo, somando juntas 83% de todo o *market share*.

Figura 2 – Gráfico divulgado por valuewalk.com market share dos SGBDRs



Fonte: Shukla (2014)

Os dados foram gerados pela IDC, empresa de inteligência de mercado e consultoria nas indústrias de tecnologia da informação. Ela atua analisando predizendo as tendências tecnológicas para que os profissionais, investidores e executivos possam tomar decisões de compra e negócios nestes setores. É uma consultoria respeitada que atua a mais de cinquenta anos no mercado.

Baseados nestes dados, este trabalho vai apresentar o que cada uma destas empresas apresenta como soluções para manter alta disponibilidade no seu principal SGBDR.

Oracle:

De acordo com o site da Oracle ([s.d.]) são apresentadas as seguintes soluções:

- Oracle Real Application Cluster (RAC): Trata-se de um *cluster* no nível dos servidores de instância de banco de dados, permitindo múltiplas instâncias a acessar o mesmo banco em um *storage* comum ao mesmo tempo. A comunicação entre os nós é feita através de uma rede de alta velocidade chamada de *interconnect*.
- Oracle Active dataguard: *Cluster* ativo/passivo que permite o *failover* de instância no caso de falha do nó principal. Entende-se por *failover* o processo de mover recursos entre os nós de um *cluster* no caso de um deles apresentar falhas.
- Oracle GoldenGate – Solução de replicação de dados específicos de um ou mais bancos de origem para um banco de destino. Apresenta outras funcionalidades que não estão relacionadas a alta disponibilidade.

IBM (DB2):

De acordo com o site da IBM ([s.d.]) são apresentadas as seguintes soluções:

- DB2 High Availability Disaster Recovery (HADR): Uma solução onde são mantidos dois bancos de dados, cada um deles em um servidor normalmente em prédios diferentes para fim de recuperação de desastres. O servidor principal executa as operações e requisições da aplicação, enquanto o outro servidor mantém uma cópia do banco, conhecido como *Standby*. Os *logs* das operações realizadas no servidor principal são enviados para o *standby* onde as mesmas operações são aplicadas, mantendo a sincronia entre os dois bancos. Em caso de falha do principal, o *standby* pode assumir os serviços em questões de minutos.
- IBM® DB2® pureScale®: De maneira parecida com o Oracle RAC, nesta solução existe mais de um SGBDR instalados em múltiplos servidores, chamados de membros com acesso a banco de dados por um *storage* compartilhado.

De acordo com o site da Microsoft ([s.d.]) são apresentadas as seguintes soluções:

Microsoft (SQL Server):

- AlwaysOn Failover Cluster Instances: Solução que mantém múltiplas instâncias de banco de dados, cada uma rodando em um servidor diferente. Somente uma das múltiplas instâncias de um banco consegue acessar os dados por vez, e acontece um *failover* para outra instância do *cluster* no caso de falha da instância primária.

Em uma breve comparação entre as soluções de cada um dos provedores citados acima, as que têm maior potencial de manter 100% da operabilidade do SBGDR com o menor tempo de indisponibilidade são o ORACLE RAC e o DB2 PureScale, visto que são *clusters* do tipo ativo/ativo . Durante o tempo de *failover* em clusters ativo/passivo, temos alguns instantes de indisponibilidade enquanto o acesso aos arquivos de banco são movidos entre as instâncias do banco.

Já na solução utilizando RAC e DB2 *PureScale*, têm-se tipicamente dois ou mais servidores, cada um com uma instância de banco de dados acessando o mesmo banco ao mesmo tempo. No caso de falha de uma das instâncias, o serviço continua disponível nos outros servidores remanescentes.

O Oracle RAC se mostra mais eficiente que o *DB2 PureScale* já que atualmente somente ele é capaz de fazer o *failover* das sessões de usuários que estão ativas no nó defeituoso. Entende-se por sessão, as conexões dos usuários na instância de banco de dados.

No próximo capítulo, será mostrada uma solução de alta disponibilidade para banco de dados utilizando o *Oracle Real Application Cluster* (RAC) que tem potencial de 100% de disponibilidade e pertence ao produto com o maior *market share* atualmente.

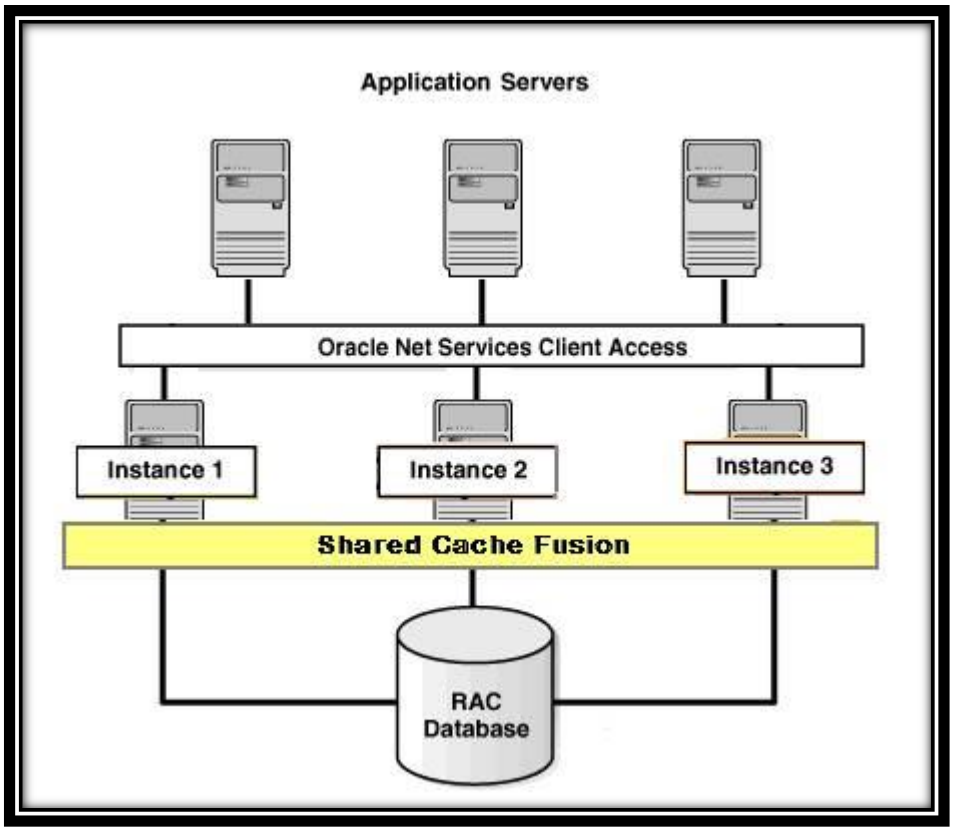
6 ORACLE REAL APPLICATION CLUSTER (RAC)

Segundo a descrição do produto no site da Oracle ([s.d.]) :

> “O Oracle Real Application Clusters (Oracle RAC) é uma versão em cluster do Oracle Database com base em uma pilha de alta disponibilidade abrangente que pode ser usado com o fundamento de um sistema em nuvem de banco de dados, bem como uma infraestrutura compartilhada, o que garante alta disponibilidade, escalabilidade e agilidade”.

A Figura 3 a mostra a arquitetura básica de um ambiente utilizando o RAC:

Figura 3 – Ilustração de um ambiente utilizando RAC



Fonte: Lascon Storage ([s.d.])

Como mostrado na figura 3, RAC é uma implementação de *cluster* no acesso ao banco de dados, contando com uma infraestrutura que possibilita mais de uma instância de banco, instaladas através de mais de um servidor, capazes de atender as requisições destinadas ao banco de dados.

A seguir, serão apresentados cada um dos componentes que fazem parte de uma estrutura RAC de acordo com o Oracle White Paper (2010):

Storage compartilhado*:* Para possibilitar o múltiplo acesso ao banco por mais de uma instância, é preciso que o *storage* seja compartilhado. Para tal, pode se adotar NAS (*Network attached Storage*), SAN (*storage area network*) ou discos SCSI. Todas estas tecnologias têm condições de permitir acesso a discos de maneira compartilhada. É neste *storage* compartilhado que ficaram os arquivos que compõem o banco de dados.

Interconnect: Um cluster exige uma segunda rede privada normalmente conhecida como interconexão. A interconexão é usada pelo cluster para o envio de mensagens entre os nós. A interconexão também é usada pelo Oracle RAC para implementar a tecnologia de *cache fusion*. É recomendado o uso de uma rede de alta velocidade para o *interconnect*.

Um ou mais servidores de SGBDR: O RAC Suporta até 100 servidores em *cluster*. Todos os servidores que compõem o *cluster* devem ter o mesmo sistema operacional, a mesma versão do Oracle SGBDR e suportar a mesma arquitetura, como por exemplo, 32 ou 64 bits.

Um sistema de arquivo e gerenciador de volumes: É necessária a utilização de um sistema de arquivos e de gerenciador de volumes que leve em consideração o ambiente compartilhado. A Oracle recomenda o uso do ASM que é um gerenciador de volume dinâmico e um sistema de arquivos de uso geral.

Infraestrutura de grade (*Oracle Clusterware*): A infraestrutura em grade são os *softwares* necessários fora do Banco de dados Oracle que fornecem a infraestrutura de cluster necessária para o RAC, como o *sotfware* de gerenciamento de volume, sistemas de arquivos e gerenciamento de *cluster*.

Endereços VIP (*Virtual Internet Protocol*): O RAC exige um endereço virtual para cada um dos servidores do *cluster*. O endereço de IP virtual é um endereço não usado na mesma sub-rede da rede local que será utilizado para conexão da aplicação com o banco de dados. A utilização do virtual IP existe pois se uma das instâncias de algum dos servidores que compõem o RAC ficar indisponível, acontece a migração desse endereço para outro servidor do *cluster*, redirecionando de maneira rápida as futuras conexões com o banco de dados.

Single Client Access Name (SCAN) : Para simplificar o acesso do cliente ao banco de dados do Oracle RAC, o SCAN fornece um nome único para ser usado em

solicitações de conexão do cliente que não é alterado no caso de qualquer um dos nós do *cluster* mudar ao longo do tempo.

6.1 Funcionamento básico do RAC

Na figura 4, pode-se ver que os usuários vão se conectar a uma das instâncias de banco de dados de maneira remota, através da rede. As requisições de conexão feitas pelos usuários, geralmente vindas de um servidor da camada de aplicação, vão chegar a um dos nós do *cluster*. As conexões que chegarem ao *cluster* vão ser direcionadas para um dos servidores que compõem o RAC de maneira sequencial, fazendo assim um balanceamento dos usuários conectados a cada um dos nós.

No caso de falha de um dos servidores, os processos necessários para atender as requisições são realocados para o nó que permanecer ativo.

Temos basicamente dois processos diretamente envolvidos em atender as requisições, um chamado LISTENER_SCAN aponta para qual servidor a requisição deve ser encaminhada, e outro chamado LISTENER_LOCAL cuida de tratar efetivamente a requisição de conexão com a instância de banco de dados.

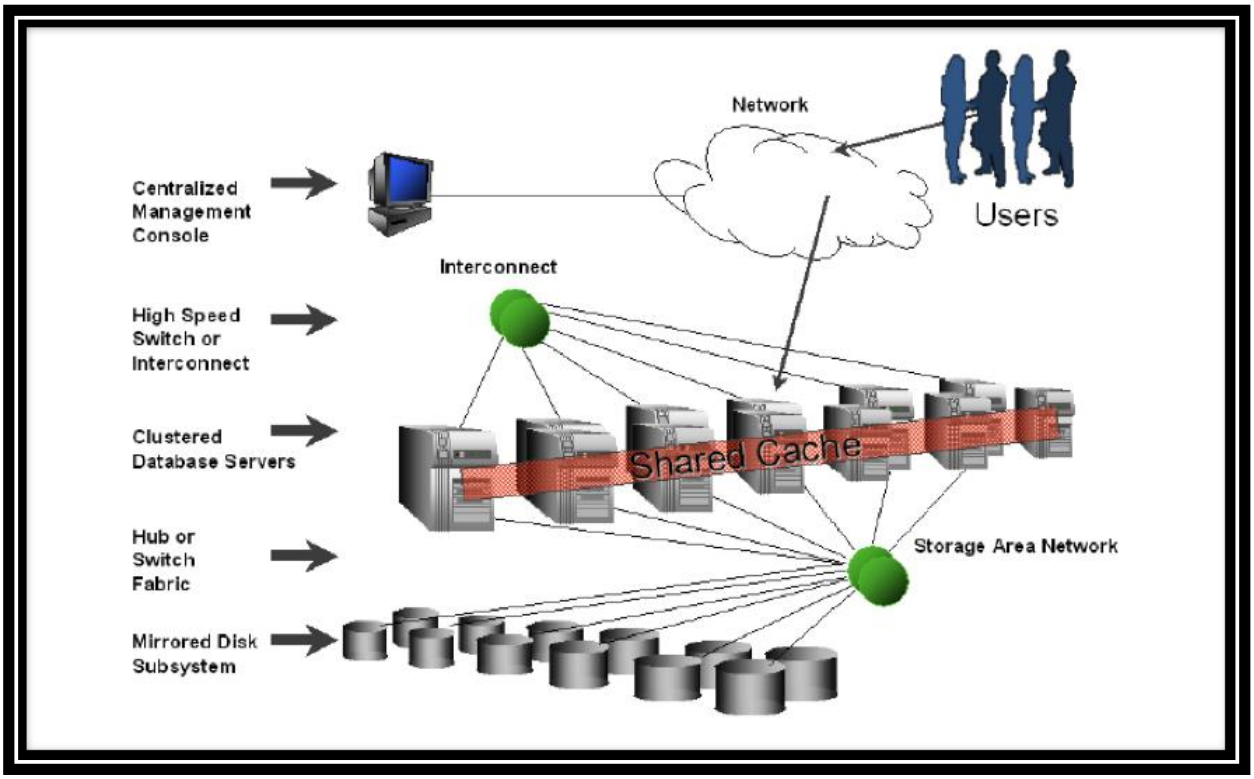
Na figura 4 também é possível ver o *interconnect*, ligando todos os nós do RAC. Aqui é onde acontece o *cache fusion*, mecanismo onde as instâncias conseguem compartilhar informações de seu *cache* local. Como exemplo, se uma instância está utilizando um bloco para efetuar sua modificação, este bloco de informação fica temporariamente travado. A instância que está travando o bloco de dados, pode enviar a informação do bloco em questão para a instância que está solicitando, utilizando o *cache* compartilhado do *interconnect*.

Por fim, observa-se o *storage* compartilhado, onde ficam efetivamente os arquivos do banco de dados. Na figura 4 está presente uma arquitetura do tipo SAN, mas outras tecnologias que permitem o compartilhamento de recursos de disco também podem ser adotadas.

A figura também indica uma *Centralized Managment console* (que se refere a uma ferramenta conhecida como *Enterprise Manager*). Esta possibilita o

gerenciamento de diversos aspectos do cluster através de uma interface *web*. Este componente é opcional e não será tratado neste trabalho.

Figura 4 – Ilustração de um ambiente RAC



Fonte: Oracle white paper (2010)

7 ESTUDO DE CASO: DISPONIBILIDADE DE ACESSO AO BANCO DE DADOS

A seguir este trabalho vai fazer uma simples demonstração de como um banco de dados continua disponível mesmo com a falha por completo de um dos seus nós. A demonstração será feita utilizando um ambiente de teste construído pelo autor, utilizando máquinas virtuais através do gerenciador Virtual BOX.

Outro objetivo é o de mostrar na prática o balanceamento de carga acontecendo entre os usuários que se conectam em um ambiente RAC através do SCAN, componente citado anteriormente.

Especificação da máquina física rodando o virtual box:

- *Thinkpad* Lenovo
- Sistema operacional Linux 64 bits, distribuição *Open Client*
- 8GB de memória.
- Processador *quad-core* Intel i5-3320M com capacidade de 2.60GHz por *core*.
- Disco de 285GB.

Especificação das duas máquinas virtuais:

- Ambas rodando Oracle Linux 64 bits;
- 1 núcleo de processamento habilitado para uso;
- 2048 MB de memória;
- 30GB de disco não compartilhado;
- 4 discos de 2,50GB de acesso compartilhado que estão sob controle do gerenciador de discos da oracle ASM;
- 2 interfaces de rede, uma em modo de rede interna utilizada como *interconnect* entre os dois nós e outra como bridge para acesso á rede pública.

Arquitetura do cenário:

Está instalado em cada uma das máquinas o gerenciador de cluster Oracle Clusterware versão 11.2.0.3.0. Há também o ASM versão 11.2.0.3.0 como gerenciador de discos compartilhados. Em cada uma das máquinas está rodando uma instância de banco de dados Oracle. Na máquina 1, chamada de rac1.ibm está

a instância de banco de dados orcl1. Na máquina 2, chamada de rac2.ibm está a instância orcl2. Ambas são instâncias do banco de dados orcl.

O cenário é composto de 3 LISTENER_SCANs, onde inicialmente o LISTENER_SCAN2 e LISTENER_SCAN3 estão ativos na máquina rac1 e o LISTENER_SCAN1 está ativo na maquina rac2.

A demonstração será realizada com uma sequencia de *screenshots.*

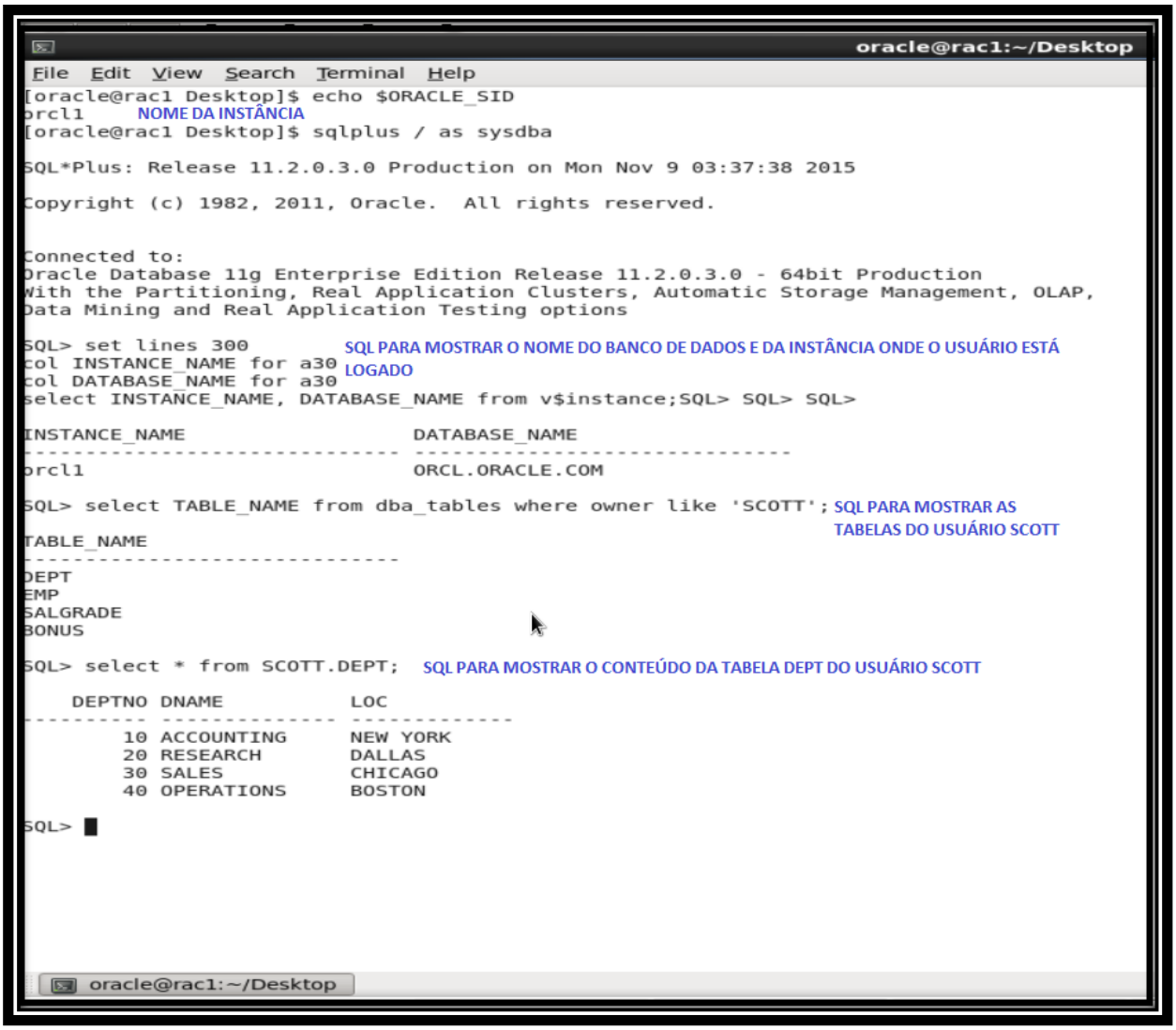
No primeiro *screenshot* está o *display* das informações de scan no ambiente. Aqui aparecem os SCANs 2 e 3 ativos no nó rac1 e o SCAN1 ativo no rac2. O comando utilizado para mostrar os scans ativos é um comando direcionado para o gerenciador do cluster e sua sintaxe é: *srvctl status scan*

Figura 5 – Disposição dos SCANs entre os 2 nós do RAC

Fonte: O próprio autor

Na figura 6 é mostrado o *logon* com privilégio de administrador do banco no servidor rac1. Aqui também é mostrado uma *SQL query* que indica qual o nome do banco e da instância onde o usuário está logado no momento. Em seguida, outra *SQL query* que mostra as tabelas do usuário SCOTT utilizado como exemplo. E por fim, uma SQL *query* que mostra o conteúdo da tabela DEPT do usuário SCOTT. Esta sequencia de *displays* tem como objetivo mostrar que tanto a instância orcl1 mostrada figura 6, quanto a instância orcl2 mostrada na figura 7 estão acessando o mesmo banco de dados orcl.

Figura 6 – *Display* de informações do usuário scott no banco orcl através da instância orcl1

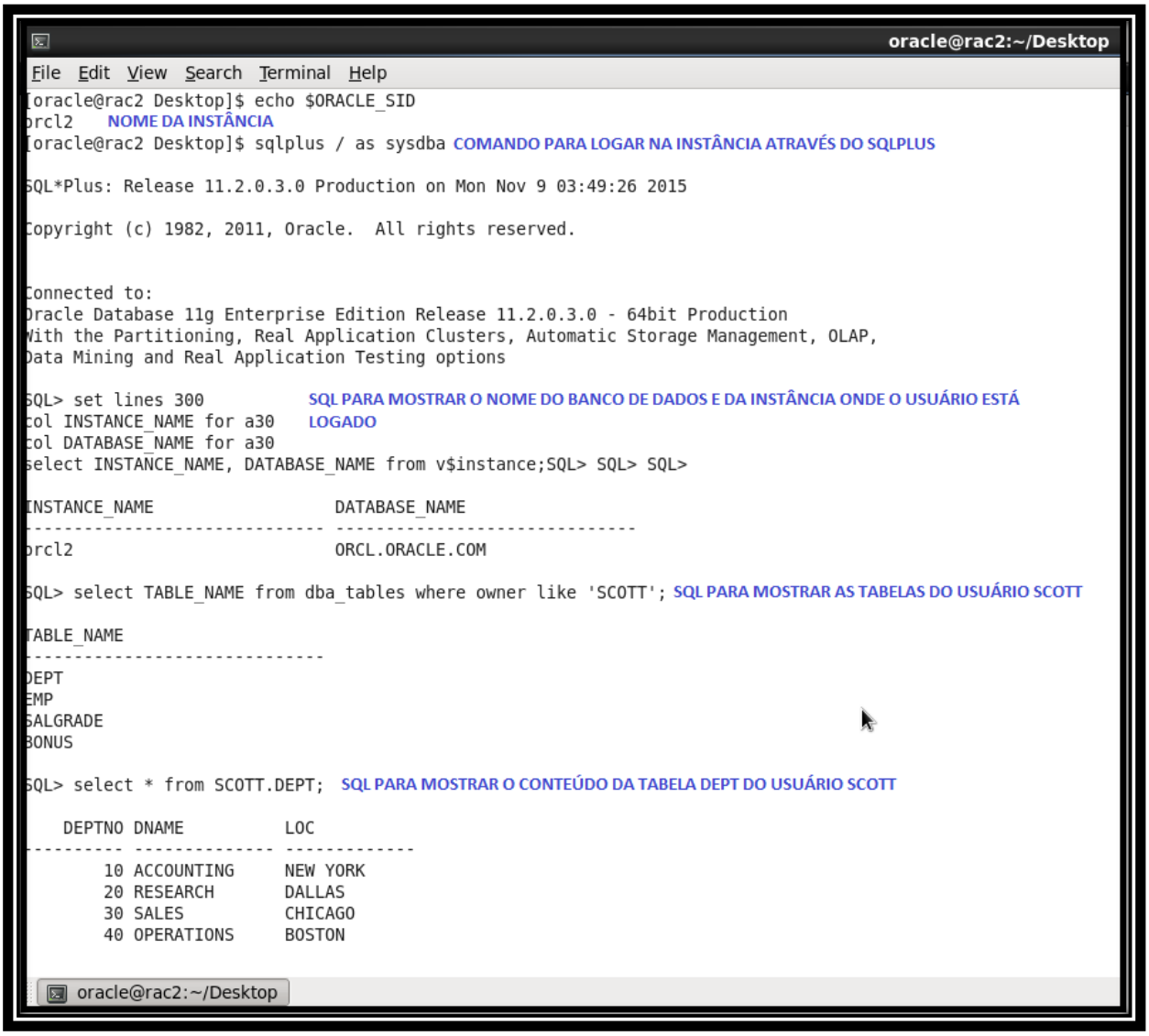


Fonte: O próprio autor

A figura 7 mostra que as mesmas informações do usuário scott do banco de dados orcl são obtidas através da instância orcl2 que está rodando no servidor rac2,

evidenciando que as duas instâncias estão acessando o mesmo banco de dados simultaneamente.

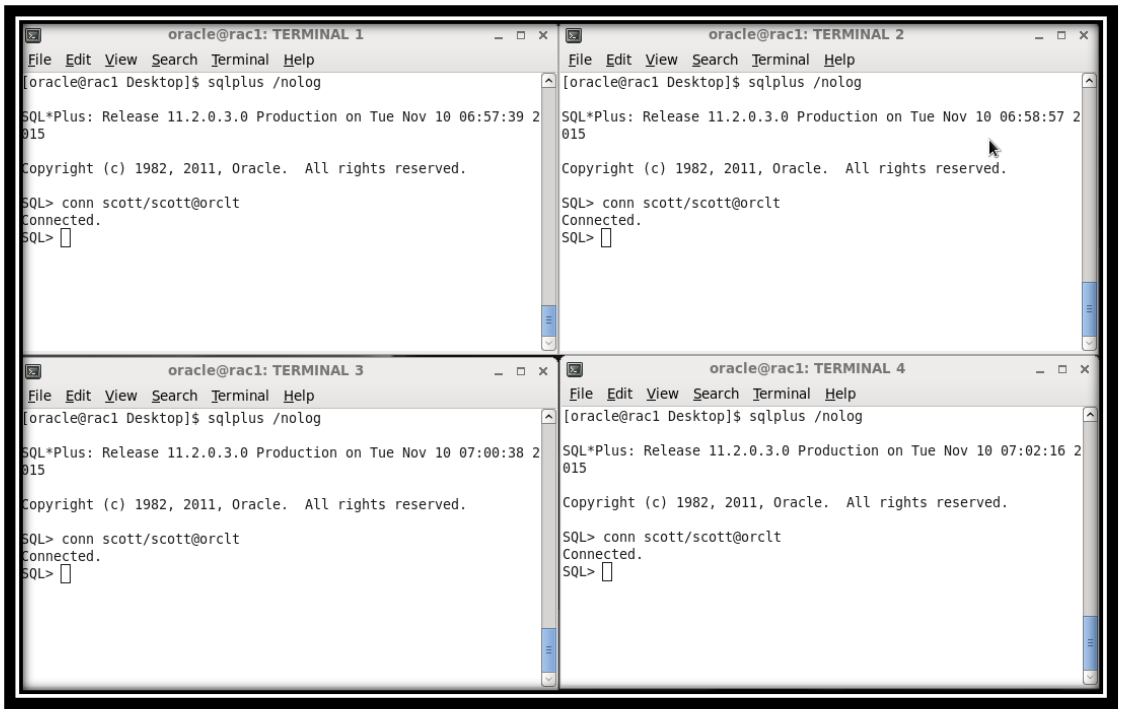
Figura 7 – *Display* de informações do usuário scott no banco orcl através da instância orcl2



Fonte: O próprio autor

Na sequência, a figura 8 mostra que foram abertos 4 terminais conectados ao banco através da string orclt. A sintaxe do comando utilizado para *logon* foi *sqlplus /nolog* para chamar o programa *sqlplus* sem se conectar a nenhuma instância. Em seguida o comando *conn scott/scott@orclt* é utilizado para se conectar ao banco de maneira remota. Desta maneira a requisição vai chegar até os LISTENER_SCANs e em seguida será direcionada para o LISTENER_LOCAL de um dos dois nós do RAC.

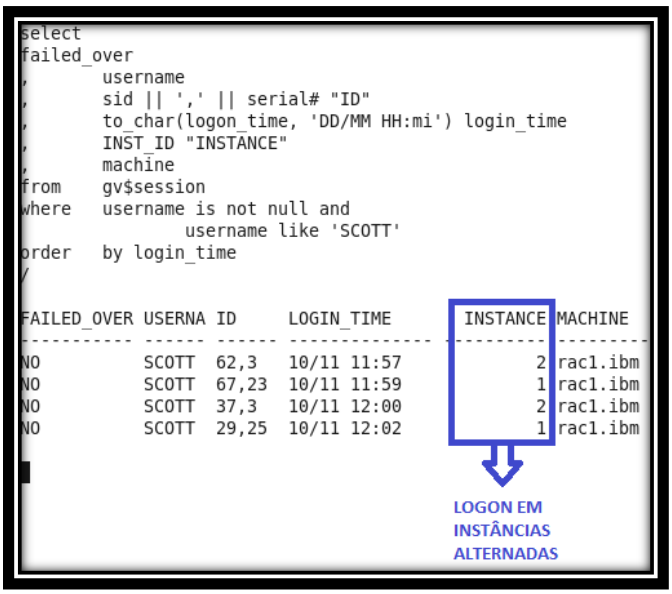
Figura 8 – Quatro terminais contactando no banco orcl



Fonte: O próprio autor

Na figura 9, foi usado um *SQL query* para mostrar que cada uma das sessões do usuário scott foram criadas alternadamente entre as instâncias orcl1 e orcl2, demonstrando o balanceamento de carga que é feito através do RAC. É possível observar que todas as sessões tem como origem a máquina rac1, porém duas delas foram direcionadas para a instância orcl1 e duas delas para a instância orcl2.

Figura 9 – Resultado dos usuários logados no banco de dados na figura 8



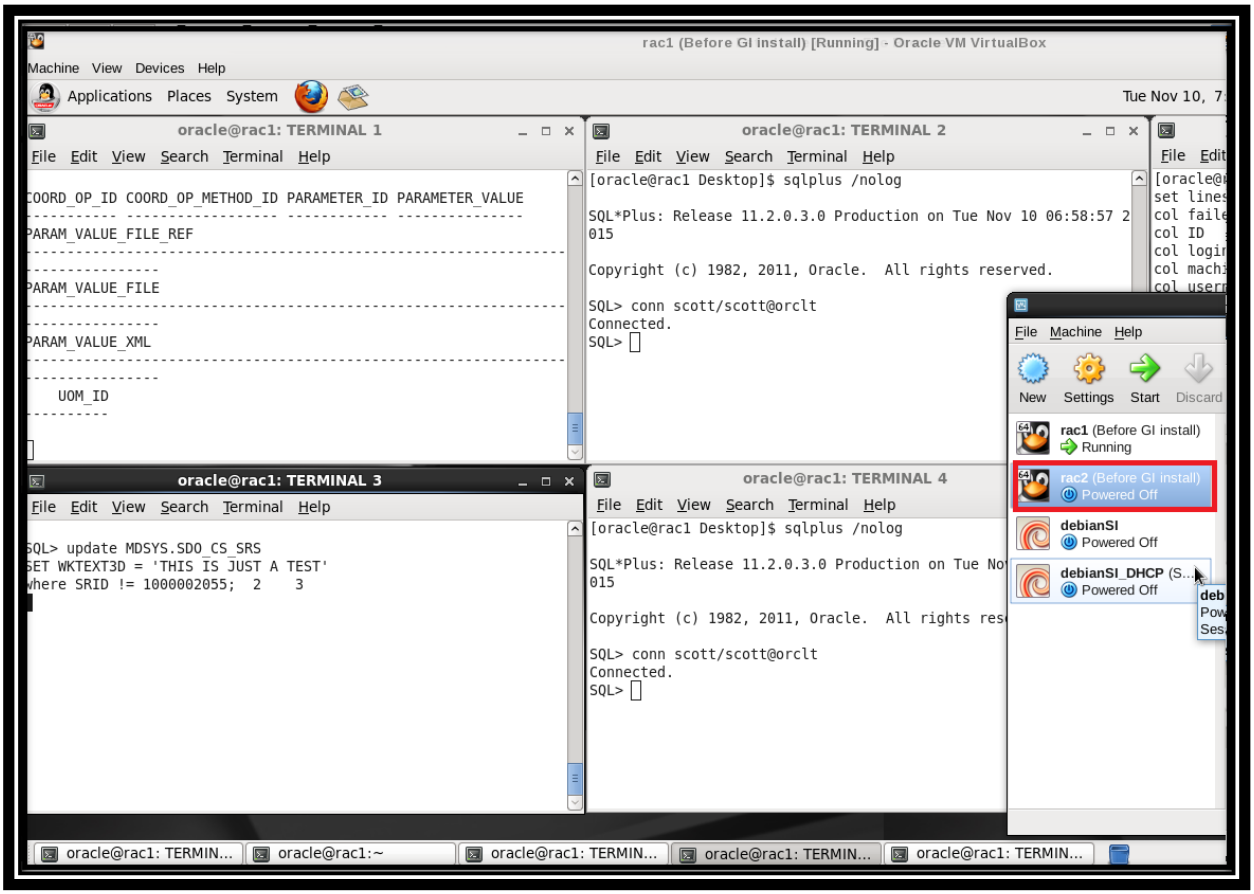
Fonte: O próprio autor

A figura 10 mostra duas operações sendo executadas. Durante a execução das operações, a máquina rac2 será desligada.

Uma das operações está no TERMINAL 1 onde foi emitida uma consulta de todos os dados da tabela MDSYS.SDO_COORD_OP_PARM_VALS. A outra está no TERMINAL 3 onde foi executado um *update* do campo WKTEXT3D para todos os registros da tabela MDSYS.SDO_CS_SRS exceto no registro que tem como campo SRID o valor 1000002055. *Update* é a operação de atualizar dados de uma tabela no banco de dados.

As operações têm como único objetivo dar uma carga de trabalho para o banco enquanto desligamos de maneira anormal a máquina rac2. O conteúdo das duas operações não tem relevância para esta demonstração.

Figura 10 – Operações rodando nos terminais 1 e 3 e máquina rac2 desligada

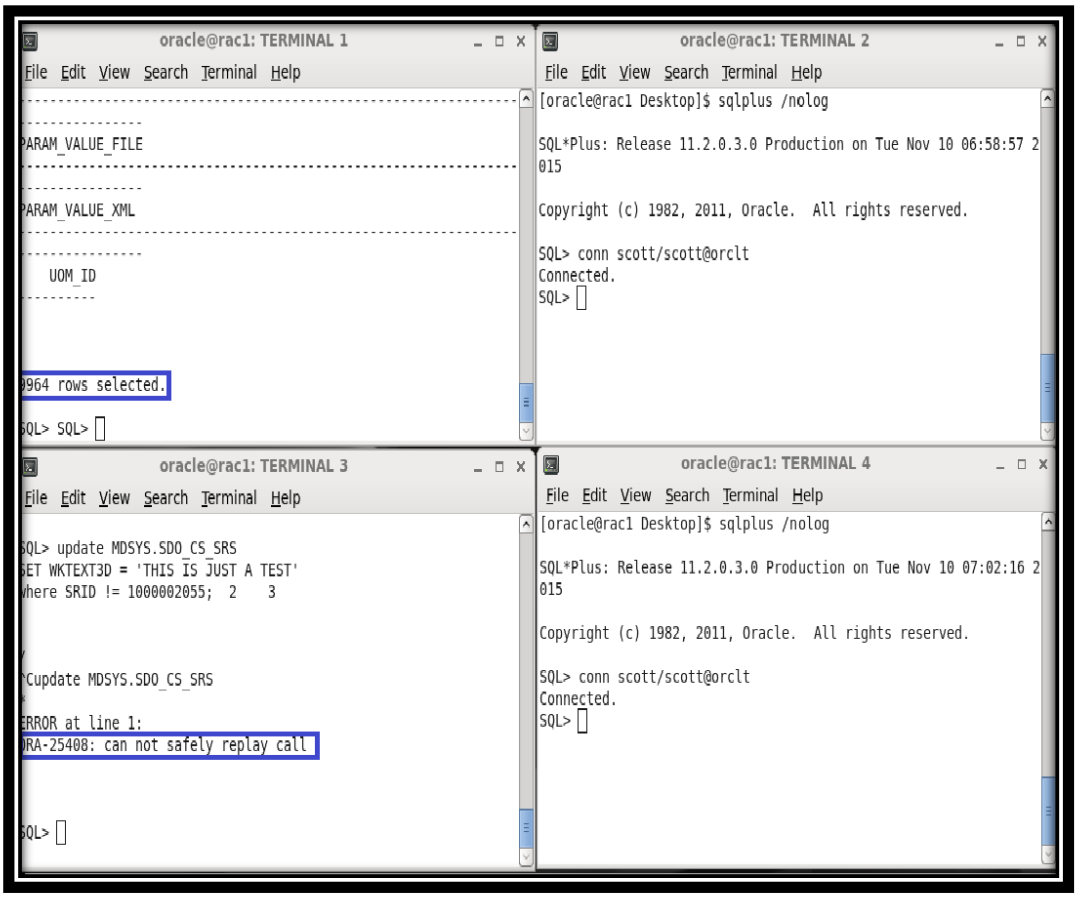


Fonte: O próprio autor

Na figura 11, o resultado das operações que estavam rodando na instância onde a máquina foi parada.

A operação de consulta no TERMINAL 1 termina sem nenhum problema enquanto o *update* no TERMINAL 3 recebe o erro ORA-25408 e as alterações são desfeitas através de *rollback*. Entende-se por *rollback* a operação de desfazer as alterações no banco de dados para o estado que estava antes de executar a modificação.

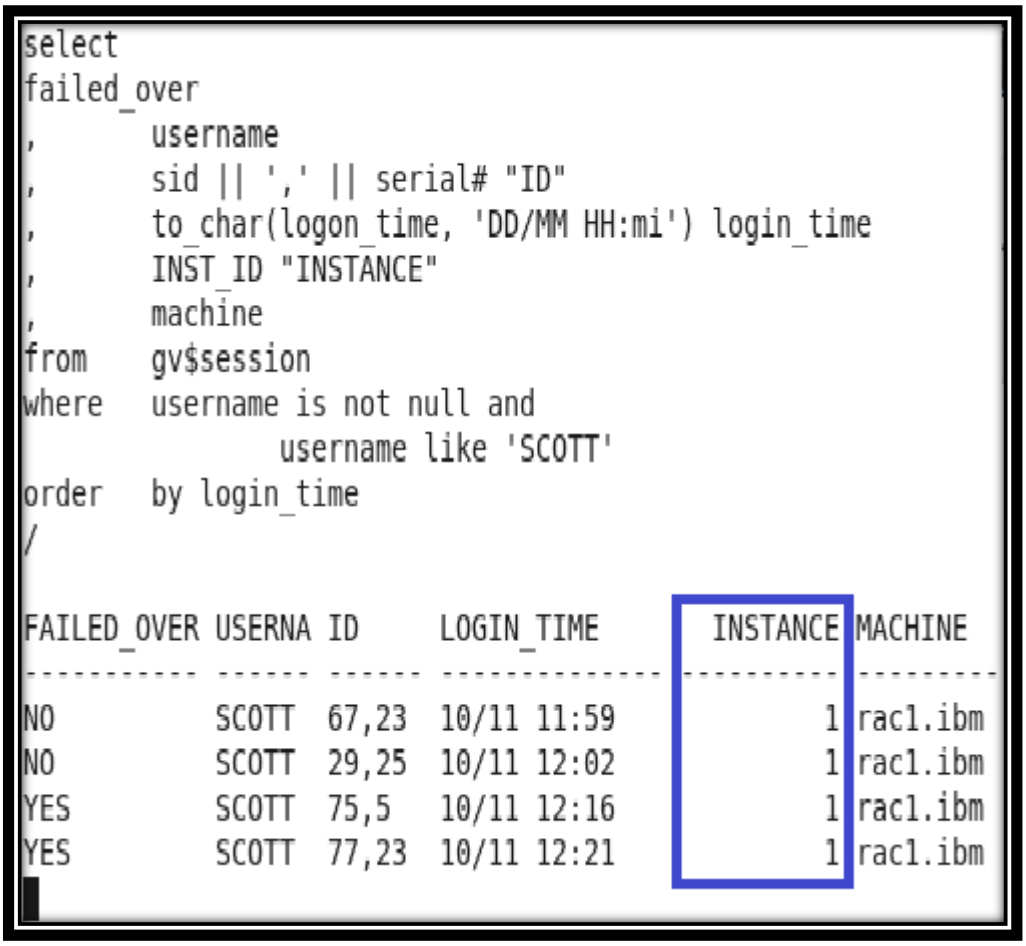
Figura 11 – Operações consulta e *update* concluindo



Fonte: O próprio autor

Na figura 12 é possível observar que as sessões que estavam conectadas no nó 2 sofreram um *failover* automático para a instância do nó 1.

Figura 12 –*Failover* das sessões da instância 2 para a instância 1



```
select
failed_over
,       username
,       sid || ',' || serial# "ID"
,       to_char(logon_time, 'DD/MM HH:mi') login_time
,       INST_ID "INSTANCE"
,       machine
from    gv$session
where   username is not null and
                username like 'SCOTT'
order   by login_time
/

FAILED_OVER USERNA ID     LOGIN_TIME      INSTANCE MACHINE
----------- ------ ------ -------------- ---------- ---------
NO          SCOTT  67,23  10/11 11:59             1 rac1.ibm
NO          SCOTT  29,25  10/11 12:02             1 rac1.ibm
YES         SCOTT  75,5   10/11 12:16             1 rac1.ibm
YES         SCOTT  77,23  10/11 12:21             1 rac1.ibm
```

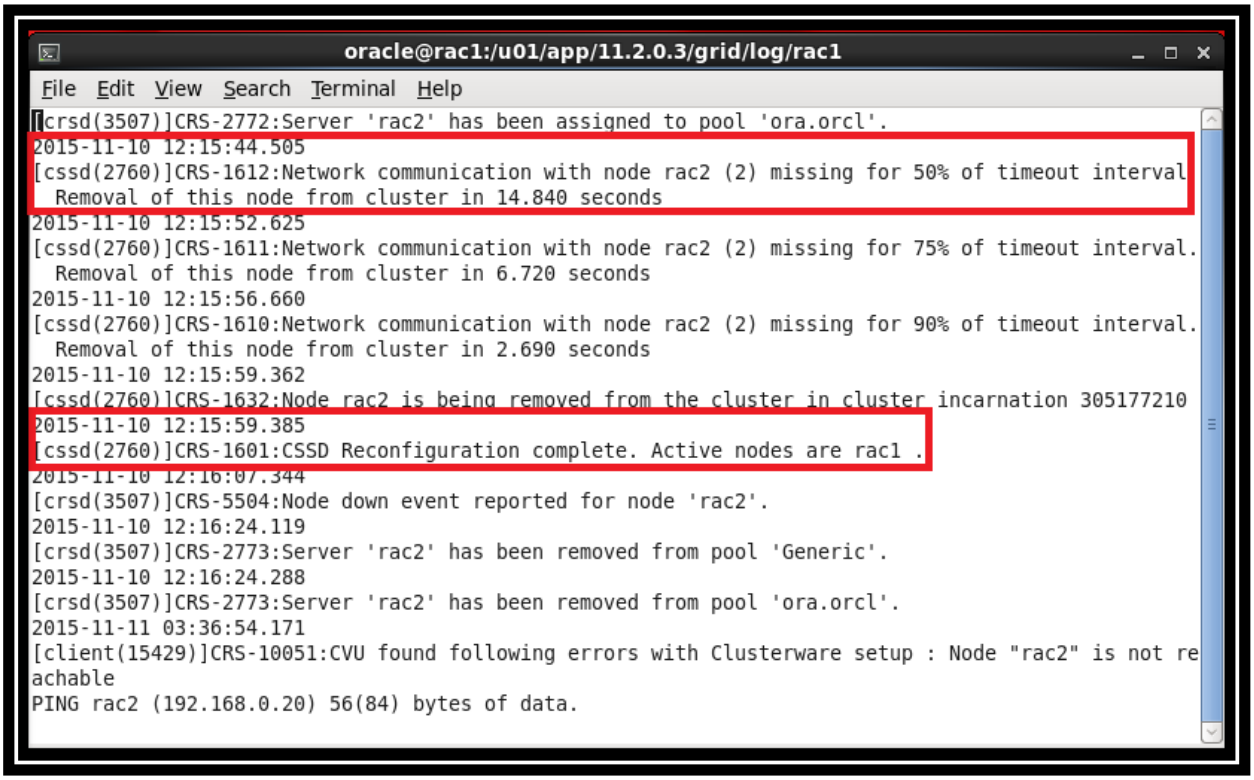
Fonte: O próprio autor

De maneira transparente para a aplicação, as sessões ativas no nó 2 foram migradas para o nó 1, mantendo 100% da disponibilidade do banco mesmo durante o desligamento da máquina 2.

Todos os serviços do *cluster* fizeram *failover* automaticamente para o outro nó, como o listener_scan entre outros, permitindo assim novas conexões com o banco de dados sem nenhum problema.

A figura 13 mostra o arquivo de log localizado no arquivo /u01/app/11.2.0.3/grid/log/rac1 contendo o momento de perda de comunicação com a máquina rac2, o momento em que a máquina rac2 é removida do *cluster* e o momento final da reconfiguração do cluster com apenas a máquina rac1 ativa.

Figura 13 – Arquivo de log mostrando reconfiguração do *cluster*



Fonte: O próprio autor

O tempo que o *cluster* espera pela retomada de conexão entre as máquinas no caso de um problema temporário de rede está definido como 15 segundos no cenário. Este tempo pode ser alterado de acordo com necessidade específica do ambiente.

- Detecção de perda de comunicação com máquina 1 ás 12:15:44 horário do *cluster.*
- Remoção da máquina rac2 da configuração ativa do *cluster* ás 12:15:59 horário do *cluster*
- Reconfiguração completa do *cluster* ás 12:15:59 horário do cluster.

Do momento do início da retirada da máquina rac2 até a completa reconfiguração do cluster passaram-se apenas cerca de 2 centésimos de segundo. É importante ressaltar que o tamanho da base de dados não tem influencia sobre o tempo de *failover* das sessões e nem no tempo de reconfiguração do *cluster,* pois a reconfiguração não lida com os dados do banco e sim com as estruturas de memória e processos das instâncias.

8 CONSIDERAÇÕES FINAIS

Com base no estudo apresentado nos capítulos anteriores, pode-se concluir que a TI tem hoje um papel de grande importância nas instituições e que a disponibilidade é um fator de grande relevância. Foi mostrado também que a alta disponibilidade de recurso de banco de dados é fundamental para aplicações críticas que precisam ficar disponíveis 24 horas por dia como as empregadas em instituições financeiras, comércios eletrônicos, empresas de produção contínua dentre outros.

Parte fundamental da tríade de segurança da informação, a disponibilidade tem papel chave na nos sistemas de informação e sem ela é impossível manter o funcionamento dos serviços pretendidos pela TI.

Como uma das alternativas para manter a disponibilidade desejada foi apresentado o produto *ORACLE RAC* que é capaz de fornecer acesso ao banco em cluster e permite *failover* no nível de sessões de usuários como visto no estudo de caso. O estudo de caso demonstrou que o RAC conseguiu fazer o *failover* a nível de sessão de usuário, mantendo a alta disponibilidade para os usuários que estavam conectados no nó defeituoso. Assim, pode-se concluir que ele é uma arquitetura que mantem alta disponibilidade no acesso ao banco de dados e pode ser empregado em ambientes de missão crítica. Para futuros trabalhos, sugere-se realizar um estudo comparativo entre a solução *ORACLE RAC* e *IBM DB2 PureScale* para destacar as principáis diferenças entre elas. Outra sugestão é estudar o funcionamento do *ORACLE RAC* em conjunto com um produto de replicação de dados como *Oracle Dataguard* ou *Oracle Golden Gate* para ter um ambiente de recuperação de desastres em um local remoto.

REFERÊNCIAS BIBLIOGRÁFICAS

BRITO, Edivaldo. **Entenda o que é RAID, técnica que torna o sistema mais rápido e seguro**. Techtudo, 29 out. 2012. Disponível em: <http://www.techtudo.com.br/artigos/noticia/2012/10/entenda-o-que-e-raid-tecnica-que-torna-o-sistema-mais-rapido-e-seguro.html>. Acesso em: 06 nov. 2015.

CANALONGA, Ricardo. **Entendendo o conceito do termo SLA**. Profissionais TI PTI, 05 ago. 2014. Disponível em: <http://www.profissionaisti.com.br/2014/08/entendendo-o-conceito-do-termo-sla/>. Acesso em: 06 nov. 2015.

DAQUINO, Fernando. **Profissão:** especialista em segurança da informação. Site Tecmundo, 16 set. 2010. Disponível em: <http://www.tecmundo.com.br/seguranca/5366-profissao-especialista-em-seguranca-da-informacao.htm>. Acesso em: 6 nov. 2015.

DIAS NETO, Arilo Cláudio. Bancos de dados relacionais. **Revista SQL Magazine 86**. Disponível em: < http://www.devmedia.com.br/bancos-de-dados-relacionais-artigo-revista-sql-magazine-86/20401>. Acesso em: 06 nov. 2015.

FONTES, Edison. **Praticando a segurança da informação**. São Paulo/SP: Brasport, 2008.

IBM. **DB2 for linux, UNIX and windows always-on transactions. Fast answers. simply delivered**. IBM, [s.d]. Disponível em: <https://www-01.ibm.com/software/data/db2/linux-unix-windows/high-availability.html>. Acesso em: 06 nov. 2015

LASCON STORAGE. **Oracle RAC**. Site Lascon Storage, 2015. Disponível em: <http://www.lascon.co.uk/Oracle-RAC.php>. Acesso em: 06 nov. 2015.

LOUREIRO, Silvana Crispim. **Segurança da informação**: Preservação das Informações Estratégicas com Foco em sua Segurança. Monografia de Pós-Graduação. Brasília: Universidade de Brasília, 2008. Disponível em: <http://dsic.planalto.gov.br/documentos/cegsic/monografias_1_turma/silvana_crispim.pdf>. Acesso em: 06 nov. 2015.

MACÊDO, Diego. **Políticas de segurança da informação**. Diego Macêdo - Analista de TI, 26 abr. 2012. Disponível em: <http://www.diegomacedo.com.br/politicas-de-seguranca-da-informacao/>. Acesso em: 06 nov. 2015.

MARQUES, Victor. **A importância da tecnologia da informação**. TI especialistas, São Paulo, 22 ago. 2014. Disponível em: <http://www.tiespecialistas.com.br/2014/08/importancia-da-tecnologia-da-informacao/>. Acesso em: 6 nov. 2015.

MICROSOFT. **Soluções de alta disponibilidade (SQL Server)**. Microsoft, [s.d]. Disponível em: <https://msdn.microsoft.com/pt-br/library/ms190202(v=sql.120).aspx>. Acesso em: 06 nov. 2015.

ORACLE. **Alta disponibilidade de banco de dados**. [s.d.]. Disponível em: <http://www.oracle.com/br/products/database/highavailability/overview/index.html>. Acesso em: 06 nov. 2015.

ORACLE WHITE PAPER. **Oracle Real Application Clusters (RAC)11g Release 2**. Documento da Oracle, Nov. 2015. Disponível em: <http://www.oracle.com/technetwork/database/clustering/overview/twp-rac11gr2-134105.pdf>. Acesso em: 06 nov. 2015.

PEREIRA, Roberto Benedito de Oliveira. **Alta disponibilidade em sistemas GNU/LINUS utilizando as ferramentas drdb, heartebeat e mon**. Monografia de Pós-Graduação. Minas Gerais: Universidade Federal de Lavras, 2005. Disponível em: <http://www.ginux.ufla.br/files/mono-RobertoPereira.pdf>. Acesso em: 06 nov. 2015.

SANCHEZ, Fabrício. **Entendendo o conceito de "storage"**. Portal GSTI, 2013. Disponível em: <http://www.portalgsti.com.br/2013/08/windows-azure-storage.html>. Acesso em: 06 nov. 2015.

SHUKLA, Vikas. **Oracle corporation (ORCL): C. Fitzgerald initiates coverage with buy**. Value Walk, 28 mar. 2014. Disponível em: <http://www.valuewalk.com/2014/03/oracle-corporation-orcl-buy-c-fitzgerald/>. Acesso em: 06 nov. 2015.

SILVA JUNIOR, Marcos Vinícius da . **O que é segurança da informação?**. Site Webinsider, 23 set. 2009. Disponível em: <http://webinsider.com.br/2009/09/23/o-que-e-seguranca-da-informacao/>. Acesso em: 6 nov. 2015.

TAURION, Cezar. **A importância da TI nas estratégias de negócio**. IDGNOW, 28 nov. 2013. Disponível em: <http://idgnow.com.br/blog/tecnologia/2013/11/28/a-importancia-da-ti-nas-estrategias-de-negocio/>. Acesso em 6 nov. 2015.