

Banco de dados

BDAV02 - Conceitos avançados

Curso Preparatório - ITnerante

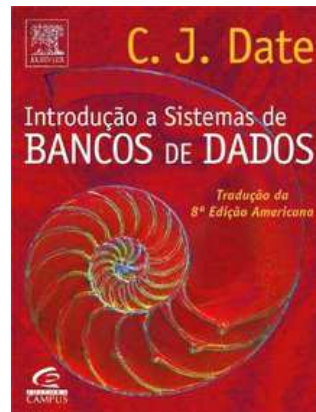
Parte 01 – Segurança de banco de dados

Parte 02 – Banco de dados paralelos e distribuídos

Prof. Thiago Cavalcanti



Bibliografia



Tire suas dúvidas

- www.itnerante.com.br
- rcthiago@gmail.com
- Lista: timasters@yahooogroups.com.br





Roteiro

- Segurança em banco de dados
 - Questões sobre segurança
 - **Controle de acesso (DAC, MAC e RCAB)**
 - Níveis de segurança
 - Injeção SQL
 - Controle de fluxo
 - Resumo sobre criptografia e certificados digitais
 - Preservação da privacidade
 - Segurança nos SGBDs comerciais: Oracle 10g



Questões sobre segurança



- Problemas:
 - Questões legais e éticas relacionadas ao **direito de acessar** certas informações
 - Questões políticas em nível governamental, institucional ou corporativo quanto aos tipos de **informações** podem se tornar **públicas**
 - Questões relacionadas ao **sistema**
 - A necessidade ou não de definir **níveis de segurança** e categorizar os dados.

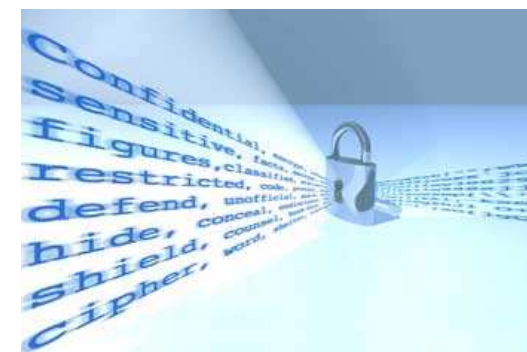


Ameaças aos banco de dados

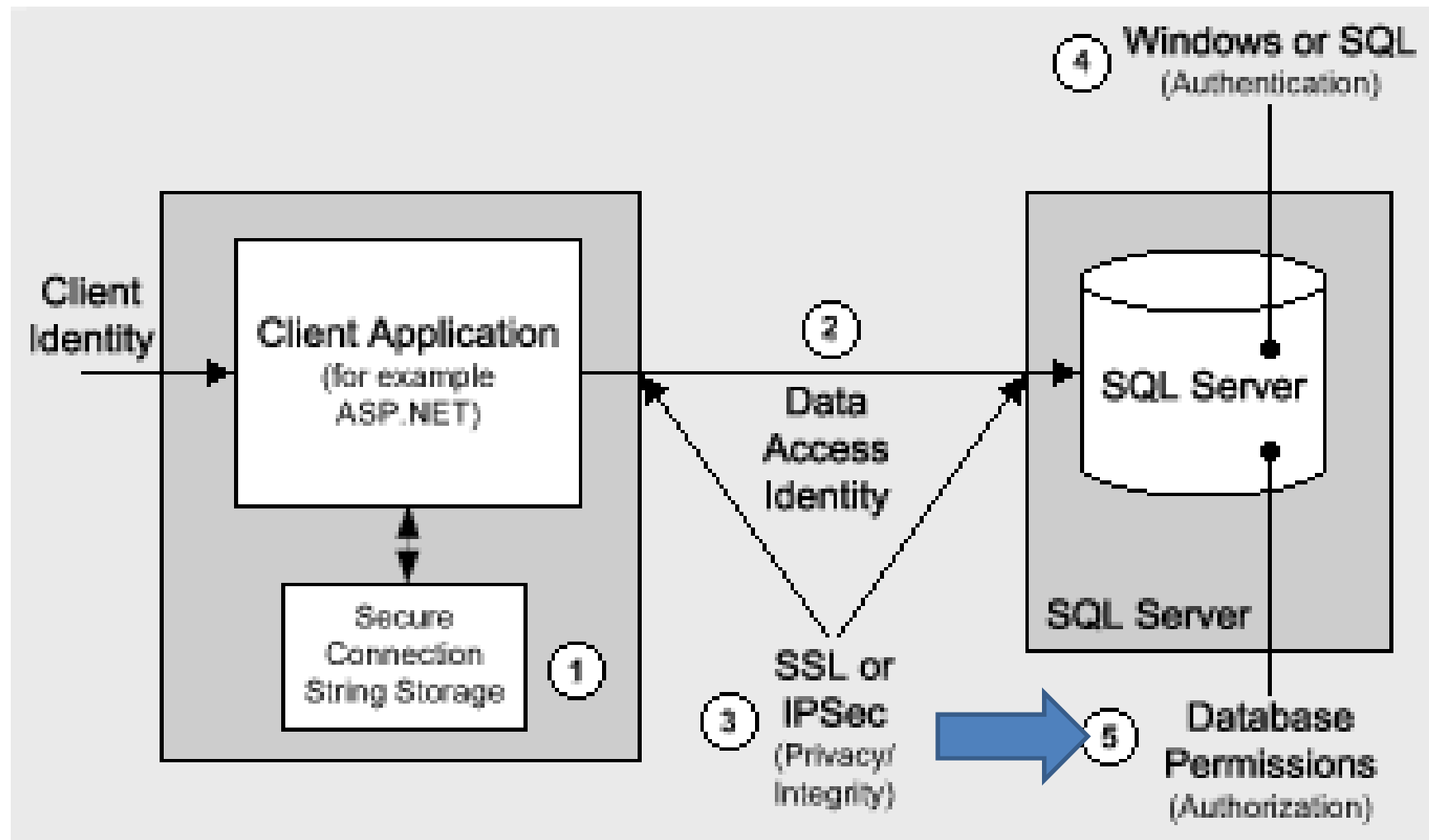


Medidas de controle

- Controle de acesso
- Controle de inferência
- Controle de fluxo
- Criptografia de dados

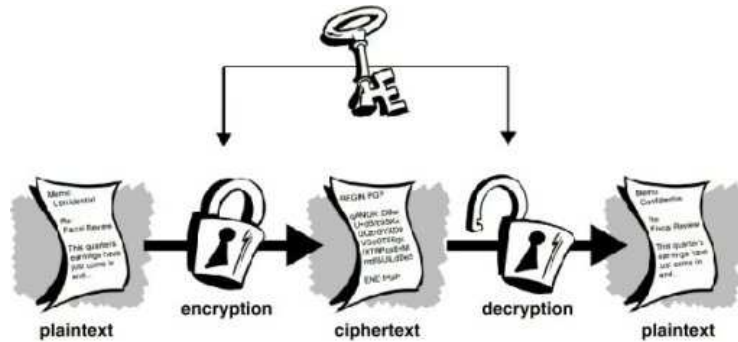


Segurança associada ao acesso aos dados



Mecanismos de seguranças em SGBDs

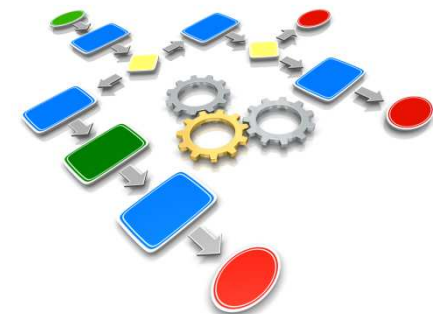
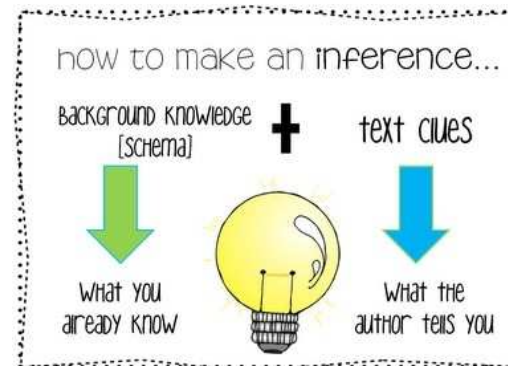
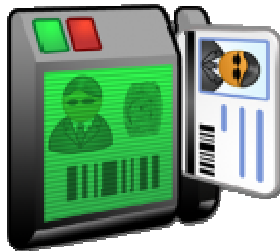
- Subsistema de segurança e autorização
 - Restringe o acesso a usuários autorizados
 - Discretionários
 - Conceder privilégios aos usuários
 - Obrigatórios
 - Impor a segurança multinível para classificação de dados e usuários em várias classes de segurança
 - Faz parte da política de segurança
 - Uma extensão do mecanismo de segurança obrigatório é a segurança baseada em papéis.



ITnerante

TIMASTERS

Medidas de controle



Controle de acesso

- Um sistema de banco de dados precisa incluir provisões para restringir o acesso ao SBD como um todo.
- Cria-se contas de usuários e senhas para controlar o processo de login pelo SGBD.



Controle de inferência

- É possível usar bancos de dados estatísticos, cujo os **dados são uma compilação ou agregação de valores** para fornecer dados agregados ao público **sem disponibilizar** dados individualmente.
- O problema é que as vezes é possível **inferir dados** sobre indivíduos específicos por meio das informações agregadas,
 - Deve ser evitado
 - Utilizamos da segurança em banco de dados estatísticos para executar tal tarefa.

Controle de fluxo

- Impedem que as informações fluam de modo a alcançarem usuários não autorizados.
- Canais secretos
 - Percursos para as informações fluírem implicitamente em caminhos que violam a política de segurança de uma organização



Criptografia de dados

- Utilizada para:
 - Proteger os dados confidenciais que são transmitidos por algum meio de comunicação
 - Proteção adicional para partes confidenciais do banco de dados



254F1	21B2C809	8833B0CC
3ECAA	CB3EE	DE038D7F
2AA4D	04143	F571C83
7DED9	B57C	820EE07
696DB	7D7F7	6DD29
0014D	41080	9754E072
05552	534146D	8360929
18BFC	0F130429	90A60B99

Segurança de BD e o DBA

- Possui **conta de superusuário** ou **conta do sistema**
- DBA - Administrador de Banco de Dados
 - É a autoridade central para gerenciar um SGBD
- Responsável por:
 - Criação de contas
 - Conceder privilégios aos usuários
 - Revogação de privilégios
 - Atribuição de nível de segurança
 - Classificar os usuários e dados de acordo com a políticas da organização
 - Auditoria do banco de dados, a partir do LOG Segurança

Controle de acesso, contas de usuários e auditorias de banco de dados



Database Instance: orcl.us.oracle.com > Logged in As SYSTEM

Users

Search
Enter an object name to filter the data that is displayed in your results set.
Object Name Go

By default, the search returns all uppercase matches beginning with the string you entered. To run an exact or case-sensitive match, double quote the search string. You can use the wildcard symbol (%) in a double quoted string.

Selection Mode:

Actions: Go

Previous 1-25 of 40 Next 15

Select	UserName	Account Status	Expiration Date	Default Tablespace	Temporary Tablespace	Profile	Created	User Type
<input checked="" type="radio"/>	ADAMS	OPEN	Oct 27, 2009 2:46:09 PM PDT	USERS	TEMP	DEFAULT	Apr 30, 2009 2:46:09 PM PDT	LOCAL
<input type="radio"/>	ANONYMOUS	EXPIRED & LOCKED	Apr 17, 2009 10:30:01 AM PDT	SYSAUX	TEMP	DEFAULT	Apr 17, 2009 10:09:42 AM PDT	LOCAL
<input type="radio"/>	APEX_PUBLIC_USER	EXPIRED & LOCKED	Apr 17, 2009 10:30:01 AM PDT	USERS	TEMP	DEFAULT	Apr 17, 2009 10:21:43 AM PDT	LOCAL
<input type="radio"/>	APPQOSSYS	EXPIRED & LOCKED		SYSAUX	TEMP	DEFAULT	Apr 17, 2009 10:06:26 AM PDT	LOCAL
<input type="radio"/>	DI	EXPIRED & LOCKED	Apr 25, 2009 12:52:18 AM PDT	USERS	TEMP	DEFAULT	Apr 25, 2009 12:48:44 AM PDT	LOCAL
<input type="radio"/>	BLAKE	OPEN	Oct 27, 2009 2:46:24 PM PDT	USERS	TEMP	DEFAULT	Apr 30, 2009 2:46:24 PM PDT	LOCAL

DBA

- Activity Report

Start Date: 2012-06-09 18:03:42 End Date: 2012-08-09 18:03:42

Aliases: ON ClientIPLike: LIKE %

DBUserLike: LIKE % FullSQLLike: LIKE %

NetProtocolLike: LIKE % ServerIPLike: LIKE %

ServerTypeLike: LIKE %

Timestamp	Session Id	DB User Name	Event User Name	Full Sql	Full SQL ID
2012-07-25 16:39:58.0	3719	DB2INST2		SELECT 'GuardAppEvent:Released','GuardAppEventUserName:marc' FROM SYSIBM.SYSDUMMY1	50432
2012-07-25 16:39:58.0	3719	DB2INST2	marc	SELECT * FROM Creditcard	50431
2012-07-25 16:39:58.0	3719	DB2INST2	marc	SELECT 'GuardAppEvent:Start','GuardAppEventUserName:marc' FROM SYSIBM.SYSDUMMY1	50430
2012-07-25 16:39:04.0	3719	DB2INST2		SELECT 'GuardAppEvent:Released','GuardAppEventUserName:sven' FROM SYSIBM.SYSDUMMY1	50429
2012-07-25 16:39:04.0	3719	DB2INST2	sven	SELECT * FROM Creditcard	50428
2012-07-25 16:39:04.0	3719	DB2INST2	sven	SELECT 'GuardAppEvent:Start','GuardAppEventUserName:sven' FROM SYSIBM.SYSDUMMY1	50427

Expandir a entrada de log criando uma trilha para auditoria.

Dados sensíveis e tipos de exposição

- Sensibilidade dos dados
 - É uma medida de **importância atribuída** a um dado por seu proprietário, com a finalidade de indicar sua necessidade de proteção.
- Dados são confidenciais?
- Fatores para se revelar um dado:
 1. Disponibilidade de dados
 2. Aceitabilidade do acesso
 3. Garantia de autenticidade



Conceitos: Segurança x precisão

- Segurança
 - Meio de garantir que todos os dados sejam mantidos seguros contra adulteração e que o acesso a eles seja controlado de modo adequado.
 - Prover segurança significar expor apenas dados não confidenciais e rejeitar qualquer consulta que referencie um campo confidencial
- Precisão
 - Proteger todos os dados confidenciais enquanto expõe o máximo possível dados não confidenciais

Privacidade da informação

- Proteção e uso de informações pessoais?
- Dimensões filosóficas, legais e práticas
- Existe uma sobreposição considerada entre:
 1. Questões relacionadas ao acesso a recursos (segurança) e
 2. Questões relacionadas ao uso apropriado da informação (privacidade).



Controle de acesso discricionário (DAC)

- Baseado na **concessão e revogação de privilégio**
- Identificador de autorização
 - Usuário ou Conta
- Níveis de atribuição de privilégios
 - Nível de conta – neste nível o DBA especifica os privilégios que cada conta mantém independente das relações do banco
 - Nível de relação ou tabela – o DBA pode controlar o acesso a cada visão ou relação em particular.

Nível de conta

Create Schema, Create Table, Create View

- CREATE TABLE Persons (
 PersonID int,
 LastName varchar(255),
 FirstName varchar(255),
 Address varchar(255),
 City varchar(255));

Alter, Drop, Modify

- ALTER TABLE Persons
 ADD DateOfBirth date

Select

- SELECT FirstName , City FROM Persons;

Nível de relação

- São definidos no SQL2
- Para cada usuários as relações individualmente
 - Alguns privilégios podem ser dados a atributos específicos de uma relação
- Modelo de matriz de acesso
 - Cada posição na matriz representa os tipo de privilégios (leitura, escrita, atualização) para cada sujeito (usuário, conta ou programa)

Privilégios para relações individuais(R) em SQL

- SELECT em R
- Modificação em R
 - UPDATE, INSERT, DELETE
- Referências em R
 - Capacidade de referenciar uma relação R ao definir uma restrição de integridade.
- Obs.: para criar uma visão é preciso que a conta tenha o privilégio de SELECT em todas as tabelas que fazem parte da VIEW

Sobre privilégios

- Privilégios por meio do uso de visões
- Revogando privilégios
 - Comando REVOKE

```
REVOKE privilege_name  
ON object_name  
FROM {user_name | PUBLIC | role_name}
```

- Propagando privilégios
 - GRANT OPTION

```
GRANT privilege_name  
ON object_name  
TO {user_name | PUBLIC | role_name}  
[WITH GRANT OPTION];
```

- E se o privilégio for concedido por duas fontes*?

EXEMPLO

- DBA cria as contas: A1, A2, A3, A4
- DBA:
 - GRANT CREATETAB TO A1
 - CREATE SCHEMA EXEMPLO AUTHORIZATION A1;
- A1 cria as relações:
 - FUNCIONARIO e DEPARTAMENTO
- A1:
 - GRANT INSERT, DELETE ON FUNCIONARIO, DEPARTAMENTO TO A2

EXEMPLO

- A1:
 - GRANT SELECT ON FUNCIONARIO, DEPARTAMENTO TO A3 WITH GRANT OPTION;
- A3:
 - GRANT SELECT ON FUNCIONARIO TO A4;
- A1:
 - REVOKE SELECT ON FUNCIONARIO FROM A3;

EXEMPLO

- A1
 - CREATE VIEW A3FUNCIONARIO AS
SELECT Nome, Data_Nasc, Endereco
FROM FUNCIONARIO
WHERE Dnr = 5
 - GRANT SELECT ON A3FUNCIONARIO TO A3
WITH GRANT OPTION;
 - GRANT UPDATE ON FUNCIONARIO (Salario) TO A4

Limites a propagação dos privilégios

- Limitar a propagação de forma horizontal
 - Significa que uma conta que recebe o privilegio só pode **propagar para outras i contas**, no máximo.
- Limitar a propagação de forma vertical
 - Limita a **profundidade** da concessão
 - Cada vez que uma nova concessão é dada o valor da profundidade definida é reduzido em uma unidade e passado como parâmetro.

Considerações finais sobre DAC

- Políticas CAD são caracterizadas pelo alto grau de flexibilidade
 - Torna adequada a uma grande de domínios de aplicação
- A principal **desvantagem** dos modelos DAC
 - Sua **vulnerabilidade a ataques maliciosos**, como cavalos de Troia embutidos nos programas de aplicação.

Questão 01 - CESPE 2011 – Correios - Prova: Analista de Correios - Analista de Sistemas - Produção

Julgue o item abaixo

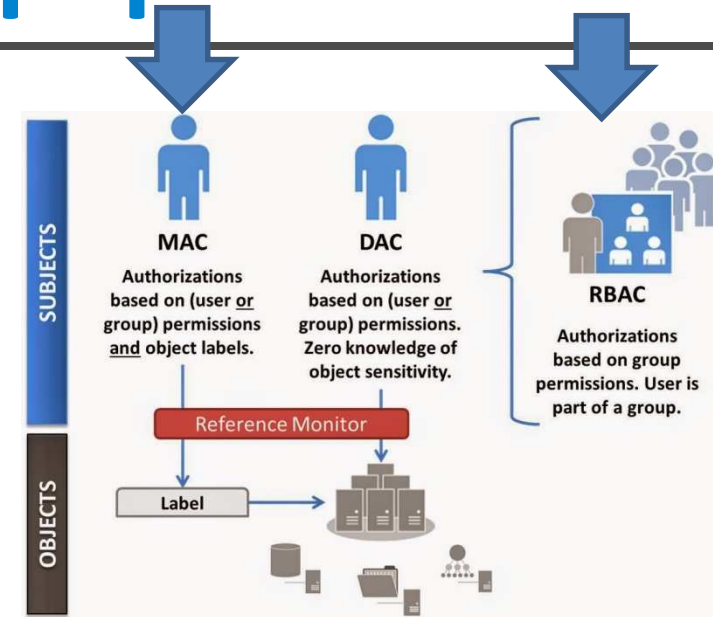
[1] Os sistemas gerenciadores de banco de dados, cujo controle de acesso é feito por usuário, não suportam o formato discricionário, pois tal formato concede privilégios associados ao usuário e aos privilégios, como a concessão de privilégio de somente leitura a determinado usuário.

Questão 02 - CESPE - 2014 Órgão: ANTAQ Prova: Analista Administrativo - Infraestrutura de TI

A respeito de segurança em banco de dados, julgue o item abaixo.

[1] A principal desvantagem dos modelos de políticas de controle discricionário em relação às políticas de acesso obrigatório é a sua vulnerabilidade a ataques maliciosos.

Controle de acesso obrigatório e baseado em papéis



Controle de acesso obrigatório (MAC)

- A necessidade de **segurança multinível** existe em aplicações do governo, militares e de inteligência, ou ainda industriais e corporativas
- Normalmente é **combinada** com mecanismos de controle **discricionários**
- **Impedem** qualquer **fluxo ilegal** de informação
- Desvantagem: Serem muito rígidas
 - Exigem uma classificação escrita entre **sujeitos** e **objetos**

Controle de acesso obrigatório (MAC)

- Classes de segurança
 - TS - Altamente confidencial (Top Secret)
 - S - Secreta (Secret)
 - C - Confidencial (Confidential)
 - U - Não classificada (Unclassified)
- Modelo ***Bell-LaPadula***
 - Sujeito
 - Objeto
 - Classificação de segurança

Restrições impostas

- Propriedade de segurança simples
 - Um sujeito S não tem permissão para acesso de leitura a um objeto O ao menos que:
 - $\text{Classe}(S) \geq \text{Classe}(O)$
- Propriedade de estrela
 - Um sujeito S não tem permissão para gravar um objeto O a menos que a $\text{classe}(S) \leq \text{classe}(O)$

Poli-instanciação

(a) **FUNCIONARIO** Tuplas originais

Nome	Salario	Desempenho	Cargo	TC
Silva U	40.000 C	Regular	S	S
Borges C	80.000 S	Bom	C	S

(b) **FUNCIONARIO** Classificação C

Nome	Salario	Desempenho	Cargo	TC
Silva U	40.000 C	NULL	C	C
Borges C	NULL C	Bom	C	C

(c) **FUNCIONARIO** Classificação U

Nome	Salario	Desempenho	Cargo	TC
Silva U	NULL U	NULL	U	U

(d) **FUNCIONARIO** Poli-instanciação

Nome	Salario	Desempenho	Cargo	TC
Silva U	40.000 C	Regular	S	S
Silva U	40.000 C	Excelente	C	C
Borges C	80.000 S	Bom	C	S

Questão 03 - FUMARC 2012 Órgão: TJ-MG Prova: Técnico Judiciário

Em relação à Segurança e Autorização em Banco de Dados, analise as seguintes sentenças, marcando (V) para verdadeira e (F) para falsa.

- () O privilégio de SELECT sobre uma relação R já permite que se estabeleça restrição de integridade referencial para R.
- () Mesmo se tiver recebido o privilégio de CREATE VIEW, um usuário ainda precisa receber o privilégio de SELECT em uma relação específica se quiser criar uma visão a partir dessa relação.
- () Um privilégio concedido com GRANT OPTION permite que o usuário que o recebeu possa conceder tal privilégio a outros usuários.
- () A concessão de privilégios não se aplica às visões.

Assinale a opção com a sequência CORRETA.

- A) V, V, F, V
- B) F, V, V, F.
- C) F, F, V, V.
- D) V, F, F, V.

Controle de acesso baseado em papeis

- Role Control Acessed Based (RCAB)
- Surgiu rapidamente nos anos 1990
 - CREATE ROLE e DESTROY ROLE
- Definir os diferentes perfis de usuários
- Os indivíduos são designados para os papeis
- Separação de papeis pode ser importante para evitar a conivência
- Hierarquia de papeis

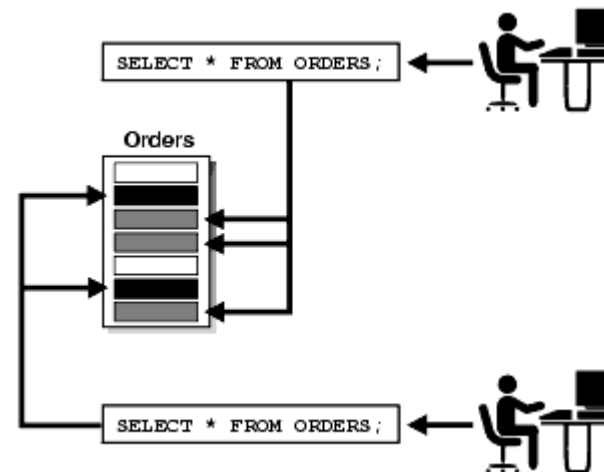
Questão 04 - FGV – 2014 - Órgão: PROCempa Prova: Analista em Infraestrutura e Redes Computacionais

Além de usuários e papéis (roles), os mecanismos de proteção e segurança de bancos de dados baseiam-se na combinação dos seguintes elementos:

- A) senhas e conexões.
- B) esquemas e bancos de dados.
- C) tablespaces e stored procedures.
- D) recursos e storage.
- E) recursos e privilégios (permissão).

Segurança baseada em rótulos

- Controle de acesso em nível de linhas
 - Cada linha de dados recebe um rótulo usado para armazenar a sensibilidade dos dados
 - Oferece maior detalhamento de segurança
 - Os rótulos são usados para que usuários vejam ou alterem certos dados



Controle de acesso para e-commerce e Web

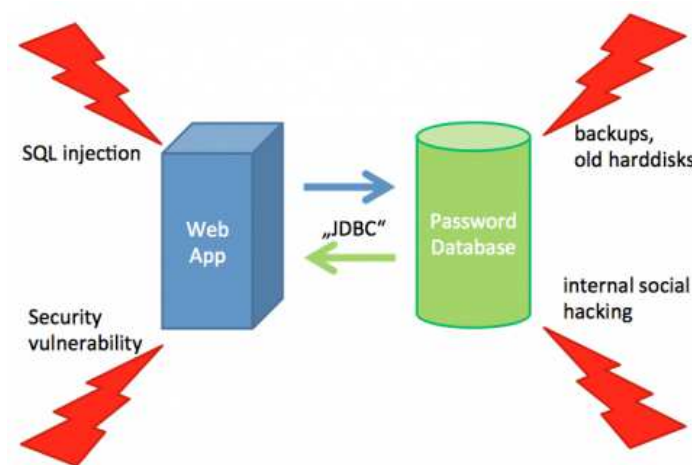
- Precisa ser flexível para dar suporte a um grande espectro de proteção heterogêneo
- Dá suporte ao controle de acesso baseado em conteúdo
- Requer políticas de controle baseadas nas características e qualificações dos usuários.
- Pode usar **credencial**
 - Um conjunto de propriedades referentes a um usuário que são relevantes para fins de segurança

Questão 05 - CESPE 2013 - Órgão: MPU Prova: Analista - Suporte e Infraestrutura

Julgue os itens subsequentes, acerca de administração de bancos de dados.

[1] A utilização de um sistema de controle de acesso mandatório é aplicável nos casos em que a estrutura de classificação de dados do banco de dados é estática.

Ataques a banco de dados



Ataques a banco de dados

- Escalada de privilégios não autorizada
 - Um indivíduo tenta aumentar seu grau de privilégios atacando pontos vulneráveis nos SBD
- Abuso de privilégios
 - Realizado por um usuário privilegiado que utiliza suas prerrogativas para danificar o banco de dados
- Negação de serviço (DoS)
 - Tentativa de tornar os recursos indisponíveis aos usuários autorizados

Ataque a banco de dados

- Autenticação fraca
 - Um usuário pode personificar a identidade de um usuário legítimo ao obter suas credenciais de login
- Injeção SQL
 - O atacante injeta uma entrada de cadeia de caracteres pela aplicação, que muda ou manipula uma instrução SQL para proveito do atacante.



Injeção de SQL

- Uma das ameaças mais comuns a um SGBD
- Métodos de injeção
 - Manipulação de SQL
 - Injeção de código (code injection)
 - Injeção de chamada de função

Manipulação de SQL

- Muda o comando SQL na aplicação
 - Por exemplo: Acrescenta condições a clausula WHERE

```
SELECT ProductName, ProductDescription  
FROM Products  
WHERE ProductNumber = 123
```

```
SELECT ProductName, ProductDescription  
FROM Products  
WHERE ProductNumber = 123 OR 1=1
```

- Incluir consultas adicionais usado UNION, INTERSECT ou MINUS

```
SELECT ProductName, ProductDescription  
FROM Products WHERE ProductID = '123'  
UNION SELECT Username, Password FROM Users
```

Injeção de código

- Tenta acrescentar instruções SQL ou comandos adicionais
- Explora um bug do computador causado pelo processamento de dados inválidos

Server Error in '/' Application.

Conversion failed when converting the varchar value 'User' to data type int.

Description: An unhandled exception occurred during the execution of the current web request. Please review the stack trace for more information about the error and where it originated in the code.

Exception Details: System.Data.SqlClient.SqlException: Conversion failed when converting the varchar value 'User' to data type int.

Injeção de chamada de função

- Uma função do bando de dados ou uma chamada a função do SO é injetada
- Usada para manipular dados ou
- Fazer uma chamada do sistema privilegiada

```
SELECT TRANSLATE (" || UTL_HTTP.REQUEST  
('http://129.107.2.1/') || ", '98765432', '9876')  
FROM dual;
```

Riscos associados à injeção SQL

- Impressão digital do banco de dados
- Negação de serviço
- Contornar a autenticação
- Identificar parâmetros injetáveis
- Executar comandos remotos
- Realizar escalada de privilégios

Técnicas de proteção contra injeção SQL

- Variáveis de ligação
 - Comandos parametrizados (PreparedStatement)
- Filtragem da entrada
 - Validação do dados
- Segurança das funções
 - Uso de função devem ser restringidas para não serem exploradas

Questão 06 - CESPE - 2014 Órgão: ANATEL - Prova: Analista Adm. - Suporte e Infraestrutura de TI

Acerca das tecnologias de segurança e dos ataques eletrônicos, julgue os itens a seguir.

[1] Os ataques de SQL Injection do tipo code injection se caracterizam por tentar modificar um comando SQL já existente mediante a adição de elementos à cláusula WHERE ou a extensão do comando SQL com operadores como UNION, INTERSECT ou MINUS.

Controle de fluxo

- Informações de um objeto mais protegido não fluem para um objeto menos protegido
- Política de fluxo
- Tipos de fluxo
 - Implícitos ou explícitos
- Canais Secretos
 - Permite que as informações passem de um nível de classificação mais alto para um nível mais baixo por meios impróprios.
 - De temporização
 - De armazenamento

Questão 07 - CESPE - 2014 - ÓRGÃO: TJ-CE - ANALISTA JUDICIÁRIO - CIÊNCIAS DA COMPUTAÇÃO

A segurança é uma área importante a ser considerada pelos administradores de bancos de dados das organizações, haja vista que a segurança visa proteger os bancos de dados contra uma série de ameaças, sejam elas advindas de usuários internos ou externos. No que se refere a esse assunto, assinale a opção correta.

- a) Uma VIEW é um mecanismo válido para que se restrinja o acesso a certos atributos de uma tabela, embora não seja possível criar restrições para um conjunto de tuplas.
- b) No controle de acesso, um usuário de banco de dados pode receber um privilégio específico sem que esteja relacionado às tabelas do banco de dados.
- c) Um usuário, uma vez que possua o privilégio de INSERT acerca de determinada tabela, não pode receber novamente o referido privilégio para a mesma tabela.
- d) Uma técnica eficiente para impedir um ataque de injeção de SQL é a utilização, ao máximo, das funções de banco de dados, em virtude desses objetos não serem alvos de ataques devido à dificuldade de se referenciá-los.
- e) Manter um registro das operações realizadas no banco de dados é uma ação suficiente para que os dados sejam protegidos contra acesso não autorizado.

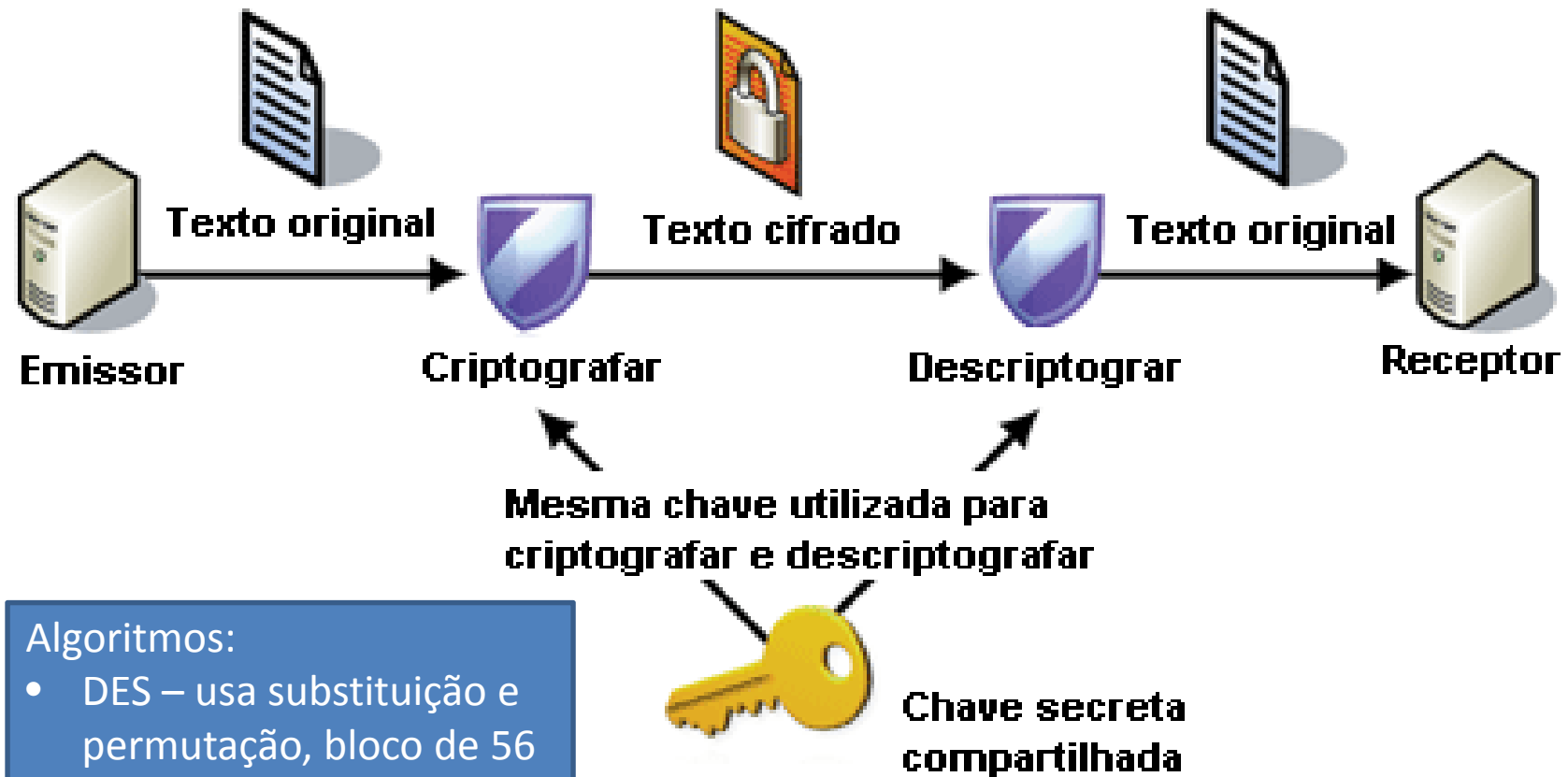
Criptografia e infraestruturas de chave pública e Segurança em Oracle

Criptografia e infraestruturas de chave pública

- Conceitos
 - Texto cifrado ou codificado
 - Texto limpo ou em claro
 - Criptografia
 - Descriptografia

A criptografia consiste em aplicar um algoritmo de criptografia aos dados usando uma chave criptográfica pré-estabelecida.

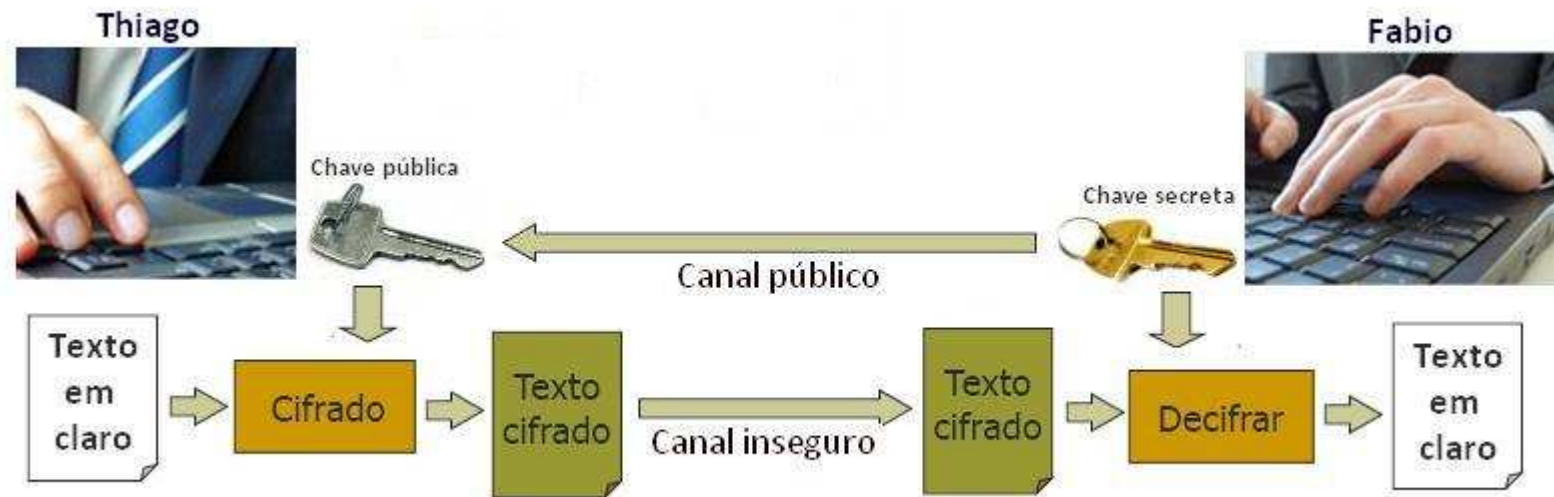
Chave simétrica



Algoritmos:

- DES – usa substituição e permutação, bloco de 56 bits
- AES – bloco de 128 bits

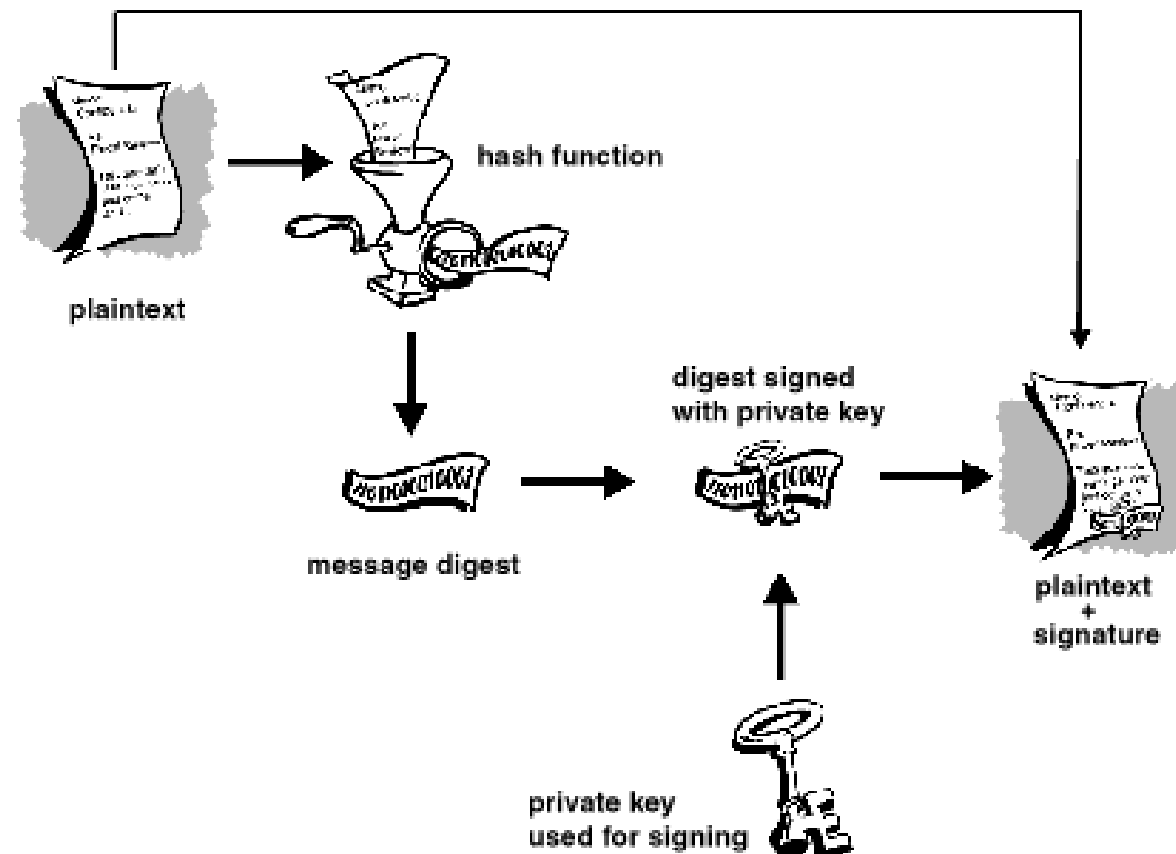
Chave assimétrica ou chave pública



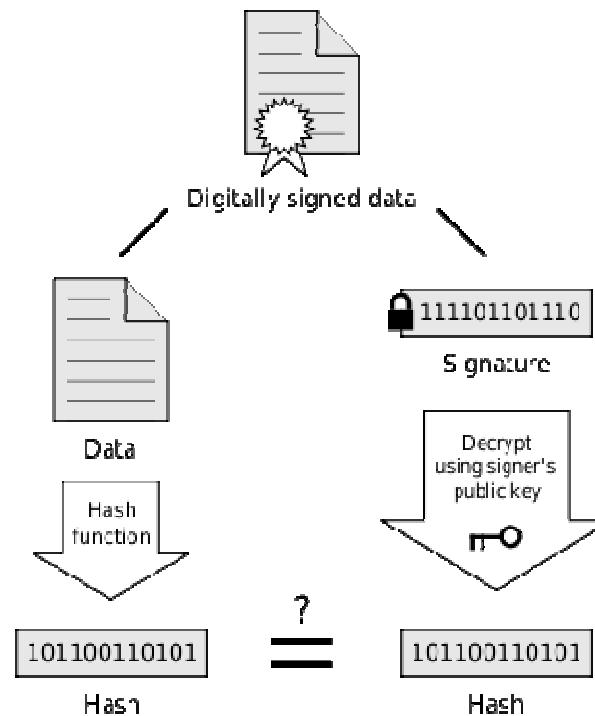
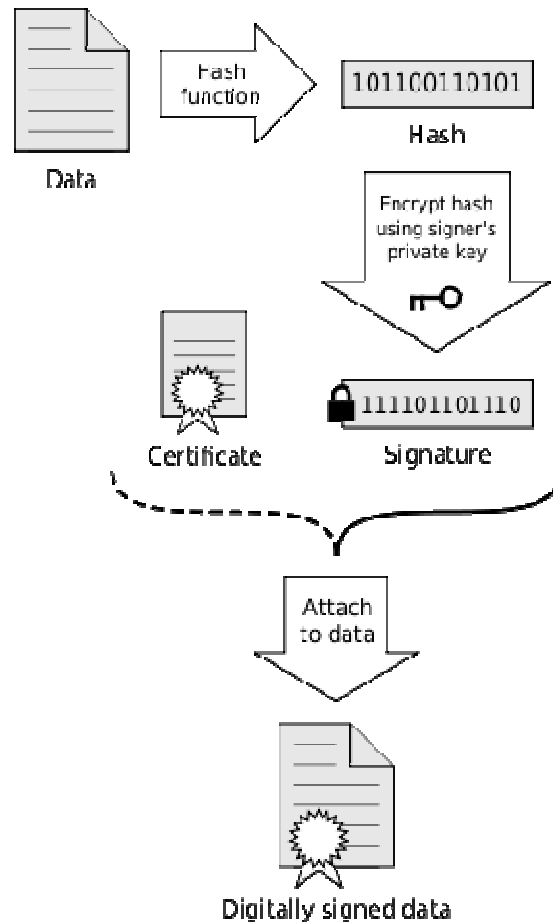
Algoritmos:

- Diffie e Hellman
- RSA
- ElGamal
- Curvas Elípticas

Assinatura digital

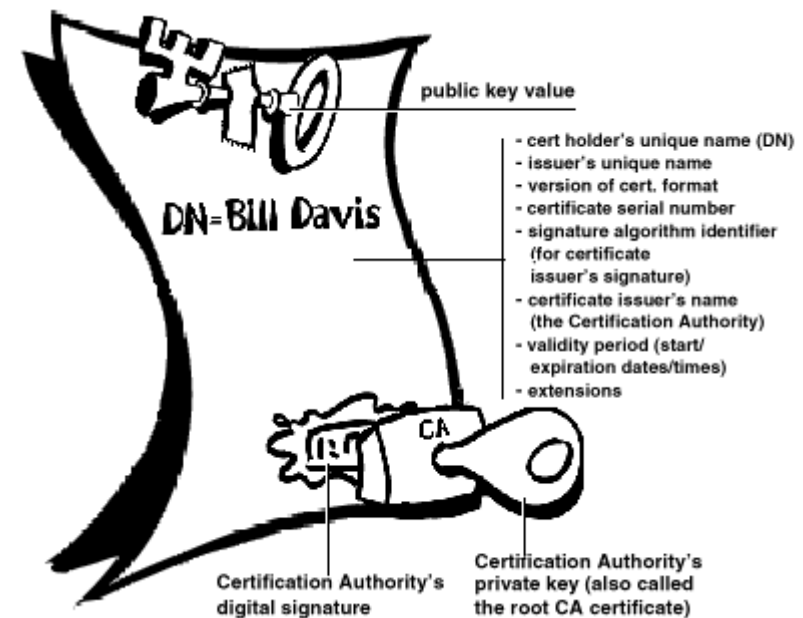


Assinatura digital



If the hashes are equal, the signature is valid.

Certificados digitais

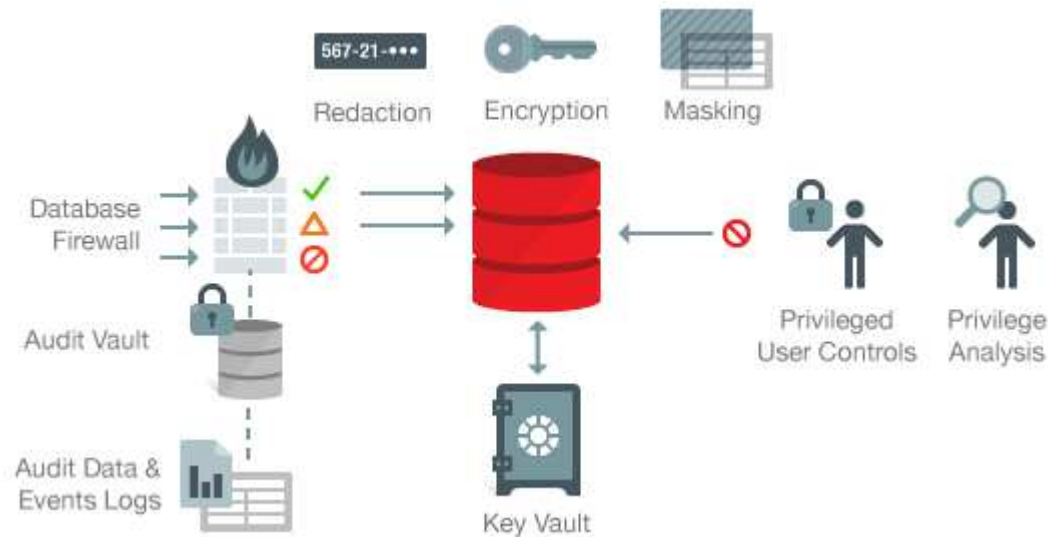


Questão 08 – FCC – 2015 -ÓRGÃO: CNMP - ANALISTA DO CNMP - SUPORTE E INFRAESTRUTURA

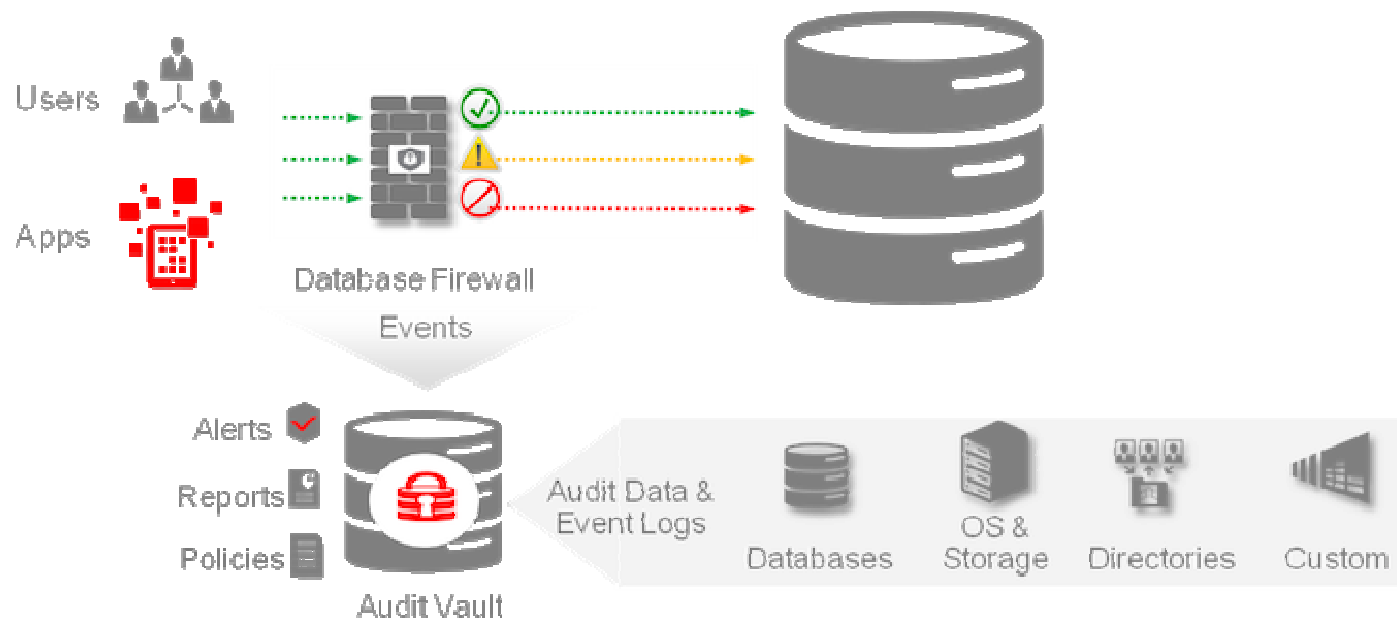
Uma das formas de se implementar a segurança em um sistema de bancos de dados é por meio da criptografia de dados, em que um dos mecanismos utilizados consiste na criptografia de chave pública, que apresenta a característica de que

- a) cada usuário do sistema de banco de dados possui apenas duas chaves públicas e nenhuma chave privada.
- b) um usuário U3 que tenha recebido dados criptografados de um usuário U4 deve conhecer a chave privada de U4 para decodificar os dados.
- c) cada usuário do sistema de banco de dados possui uma chave pública e uma chave privada.
- d) cada usuário do sistema de banco de dados possui apenas duas chaves privadas e nenhuma chave pública.
- e) se um usuário U1 quiser trocar dados com um usuário U2 deve criptografar os dados com a chave privada de U2.

Segurança em Banco de dados Oracle



Audit Vault e Database Firewall



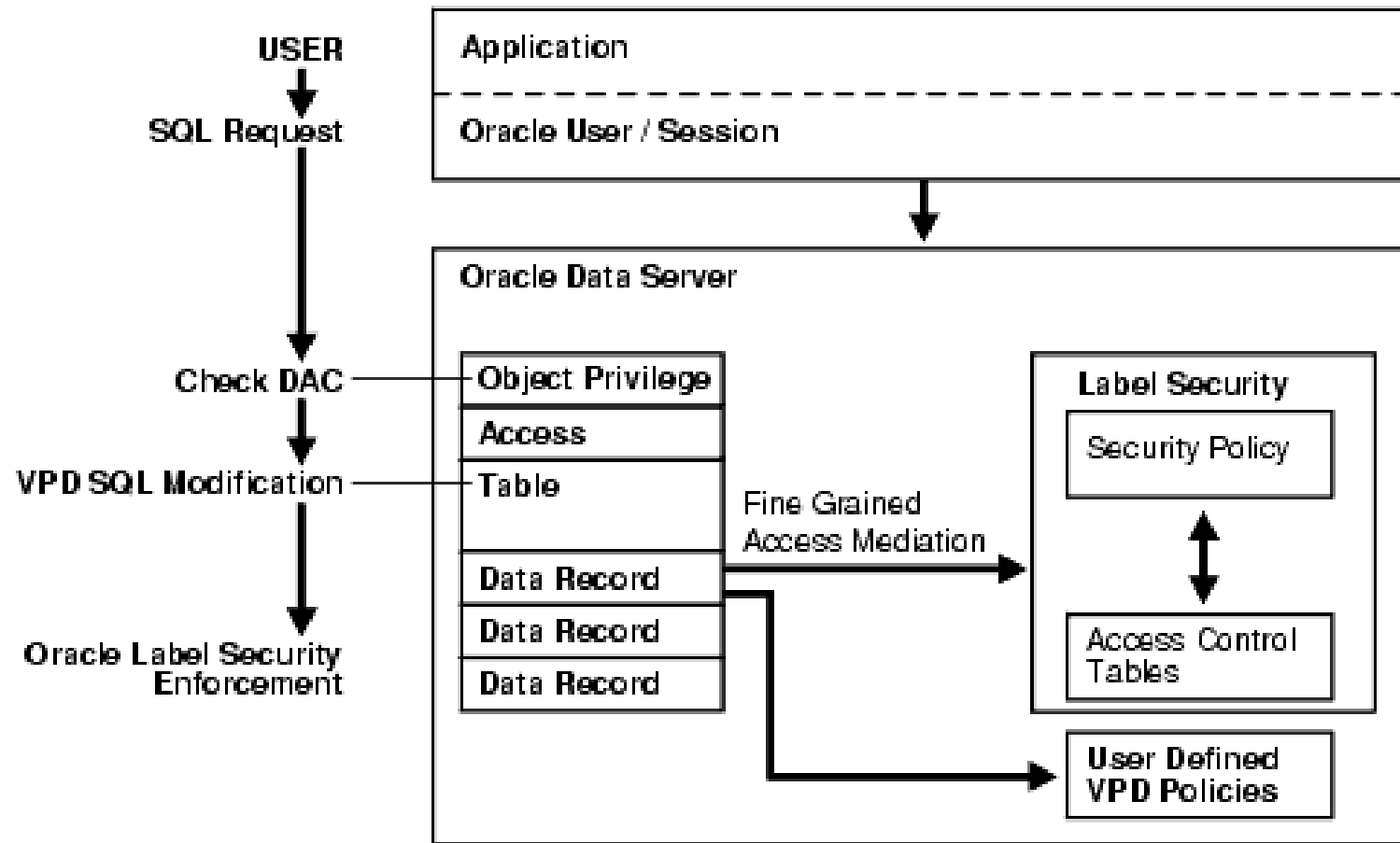
Introdução a segurança no Oracle

- Oracle Security Layer
 - Habilita o controle de acesso em nível de linha
 - Cada tabela do banco de dados tem uma política de segurança associada a ela
 - Executada toda vez que a tabela é acessada

Segurança baseada em rótulos no Oracle

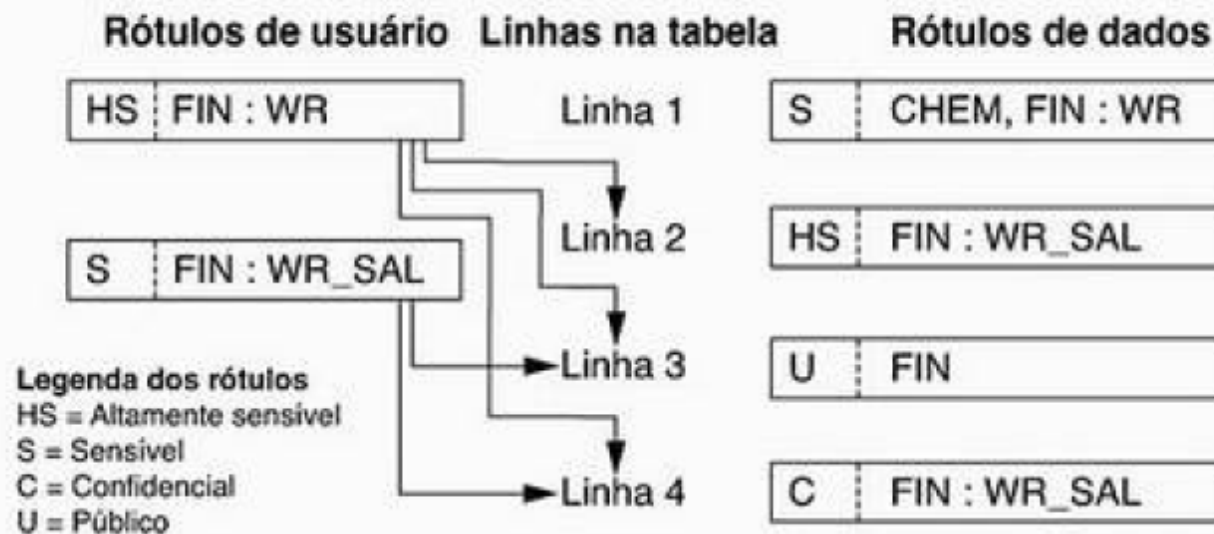
- Oferece uma forma adaptável de controlar acesso a dados confidenciais
- Tanto usuários quanto os dados possuem rótulos associados a eles
- Virtual Private Database (RAS)
 - Recurso que acrescenta predicados aos comandos dos usuários para limitar seu acesso
 - Transparente ao usuário e à aplicação
 - Permite que o desenvolvedor remova os mecanismos de segurança das aplicações e centralizem no Oracle

Arquitetura Label Security



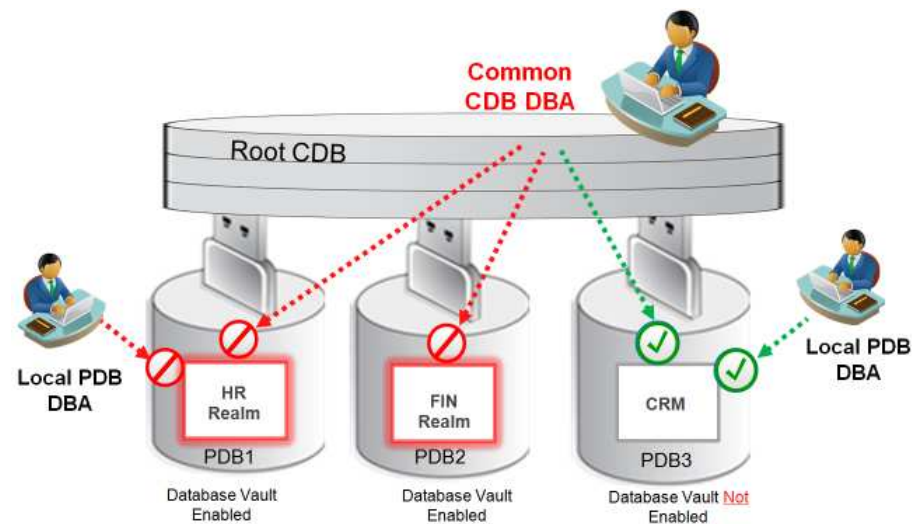
Rótulos de dados e de usuários

Rótulo de usuário	<table><tr><td>Nível de acesso máximo</td><td>Todos os compartimentos aos quais o usuário tem acesso</td></tr></table>	Nível de acesso máximo	Todos os compartimentos aos quais o usuário tem acesso
Nível de acesso máximo	Todos os compartimentos aos quais o usuário tem acesso		
Rótulo de dados	<table><tr><td>Nível de acesso mínimo exigido</td><td>Todos os compartimentos aos quais o usuário deve ter acesso</td></tr></table>	Nível de acesso mínimo exigido	Todos os compartimentos aos quais o usuário deve ter acesso
Nível de acesso mínimo exigido	Todos os compartimentos aos quais o usuário deve ter acesso		

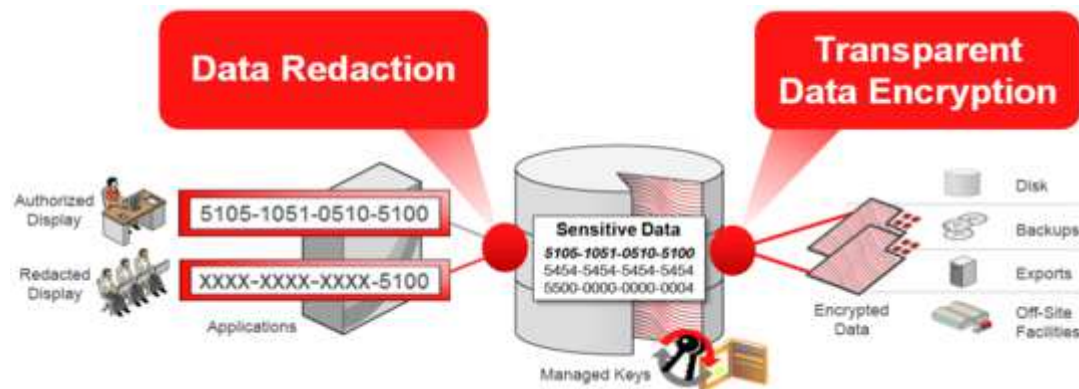


Oracle Database Vault

- Protege contra riscos internos
- Garante a privacidade dos dados
- Ajuda governantes e a indústria em relação a regulações (normas e leis)



Masking e Subsetting/ Redaction e Encryption





ITnerante 

TIMASTERS 

Simulado 01

SEGURANÇA EM BANCO DE DADOS

ITnerante 

Questão 01 - Banca: CESPE – 2011 - Órgão: Correios - Prova: Analista de Sistemas - Produção

Julgue os itens subsequentes, relativos à segurança e à integridade de banco de dados e à linguagem SQL.

[1] O uso de visão em banco de dados é uma forma de aumentar a sua segurança, pois impede o acesso direto aos dados de uma tabela, fornecendo somente os dados considerados necessários.

Questão 02 - Aplicada em: 2011 - Banca: CESPE - Órgão: Correios - Analista de Sistemas – Produção

Julgue os itens subsequentes, relativos à segurança e à integridade de banco de dados e à linguagem SQL.

[1] As restrições de domínio em um banco de dados aumentam o nível de segurança, mas não contribuem para a avaliação da integridade dos dados inseridos.

Questão 03 - Banca: CESPE - 2010 - Órgão: MPU

Prova: Analista de Informática - Banco de Dados

Em relação aos aspectos de segurança de SGBDs, julgue os itens a seguir.

[1] Considerando um modelo relacional de banco de dados, o axioma de segurança a seguir está corretamente apresentado: se o usuário *i* não tiver acesso SELECT à combinação de atributo *A*, então ele também não tem acesso UPDATE ao *A*.

Questão 04 - Banca: CESPE - 2010 Órgão: MPU - Prova: Analista de Informática - Banco de Dados

Em relação aos aspectos de segurança de SGBDs, julgue os itens a seguir.

[1] Considerando que os usuários em um sistema relacional de banco de dados recebam um nível de autorização com imposição de regras simples, é correto afirmar que as duas regras a seguir deverão ser empregadas em conjunto para evitar o fluxo ilegal de informação.

- O usuário *i* pode ver o objeto *j* apenas se o nível de autorização de *i* for maior ou igual ao nível de classificação de *j*.
- O usuário *i* só pode modificar o objeto *j* se o nível de autorização de *i* for menor que o de *j*.

TC8

Slide 76

TC8

Verificar se está faltando a figura.

Thiago Cavalcanti; 07/09/2015

Questão 05 - CESPE – 2010 - Órgão: MPU - Analista de Informática - Banco de Dados

Em relação aos aspectos de segurança de SGBDs, julgue os itens a seguir.

[1] O administrador de banco de dados deve especificar os privilégios de acesso a cada usuário ou grupo de usuários, sendo que o SGBD provê acesso seletivo a cada relação no banco de dados embasada em contas específicas.

Questão 06 - Banca: CESPE – 2010 - Órgão: MPU - Prova: Analista de Informática - Banco de Dados

Em relação aos aspectos de segurança de SGBDs, julgue os itens a seguir.

[1] Existem dois níveis de privilégio no SGBD: de conta e de relação (tabela). O primeiro independe das relações no banco de dados e o de relação refere-se ao privilégio de acesso de cada relação individual ou visão (view) no banco.

Questão 07 - Banca: CESPE – 2010 - Órgão: MPU - Prova: Analista de Informática - Banco de Dados

• Anulada

Em relação aos aspectos de segurança de SGBDs, julgue os itens a seguir.

[1] O comando SQL GRANT CREATETAB TO A1; permite criar a conta A1, a qual terá privilégios para criar base de dados.

Questão 08 - FCC - 2010 - Órgão: TCE-SP - Prova: Agente da Fisc. Financeira – Inf. - Produção e BD

Caracteriza-se pela definição de classes de segurança para os sujeitos e objetos. As classes de segurança são determinadas por duas características: o nível de classificação e a categoria. O nível de classificação reflete a sensibilidade da informação, como por exemplo: público, confidencial, secreto e ultra secreto. Já as categorias buscam refletir áreas ou departamentos das organizações. Cada objeto possui um nível de classificação e pode pertencer a mais de uma categoria, o mesmo acontecendo com os sujeitos. De forma simplificada, pode-se dizer que um sujeito poderá ter acesso a determinado objeto se seu nível de classificação for igual ou superior ao do objeto e se pertencer a pelo menos uma classe a que o objeto também pertença. Trata-se de política de controle de acesso:

- a) compulsória ou mandatária.
- b) discricionária ou provisória.
- c) discricionária ou compulsória.
- d) alternativa ou técnica.
- e) administrativa ou técnica

Questão 09 - Banca: VUNESP - 2009 - Órgão: CETESB - Prova: Analista de TI - Administração de Dados

- I. um usuário pode ter o privilégio de ler, mas não de alterar os registros de uma determinada tabela;
- II. um usuário sempre pode conceder seus privilégios a outros usuários;
- III. se um usuário puder excluir os registros de uma tabela, terá o mesmo direito sobre todas as tabelas do banco de dados.

A segurança de bancos de dados é um dos principais fatores relacionados à sua administração. Considere as seguintes afirmações sobre o controle de segurança do tipo discriminatório ou discricionário:

Sobre as funções, aquelas ligadas com aspectos de segurança são as contidas em

- a) I, apenas.
- b) II, apenas.
- c) I e III, apenas.
- d) II e III, apenas.
- e) I, II e III.

Questão 10 - Banca: CESGRANRIO - 2009 - Órgão: Casa da Moeda Prova: Analista de Nível Superior - BD

O servidor de banco de dados corporativo de uma empresa está isolado por meio de um firewall do tipo filtro de pacotes. Com base nessa informação, analise as afirmativas a seguir.

I - Tal isolamento é efetivo na proteção de ataques do tipo SQL Injection.

II - É possível bloquear o acesso de uma única estação ao banco de dados.

III - Consultas SQL excessivamente longas podem ser bloqueadas no firewall.

Está(ão) correta(s) a(s) afirmativa(s)

A) I, apenas.

B) II, apenas.

C) III, apenas.

D) II e III, apenas.

E) I, II e III.



ITnerante 

TIMASTERS 

Simulado 01

SEGURANÇA EM BANCO DE DADOS

ITnerante 

Gabarito

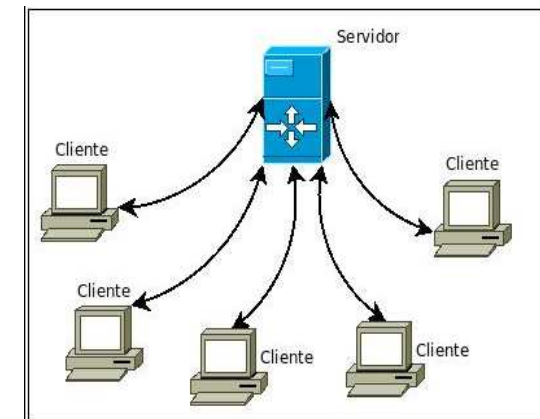
Questões de aula

1. E
2. C
3. B
4. E
5. C
6. E
7. B
8. C

Simulado 01

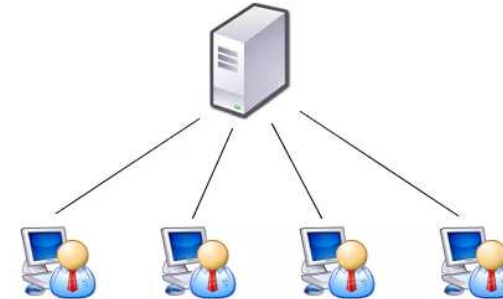
1. C
2. E
3. C
4. E
5. C
6. C
7. E (ANULADA)
8. A
9. A
10. B

Arquitetura de Sistemas de Banco de dados

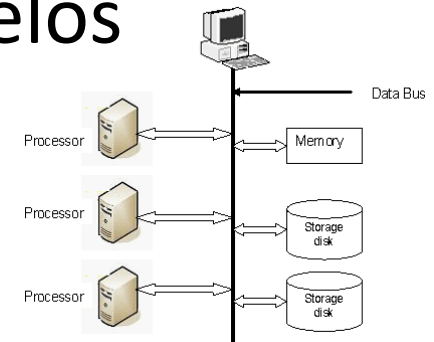


Aspectos

- Rede → Cliente-Servidor



- Paralelismo → Banco de dados Paralelos



- Distribuição → Banco de dados Distribuídos



Arquitetura centralizadas e cliente servidor

- Funcionalidade base de dados pode ser dividida em:
 - **Backend:** Gerencia as estruturas de acesso, avaliação e melhoria de consultas, concorrência e recuperação
 - **Frontend:** Consiste em ferramentas visuais tais como formulários, relatórios e ferramentas gráficas
- Vantagens de substituição dos mainframes com redes de estações de trabalho ou computadores pessoais por máquinas conectados a servidores Backend:
 - Melhor custo benefício
 - Flexibilidade na alocação de recursos e expansão das instalações
 - Melhores interfaces de usuário
 - Manutenção mais fácil

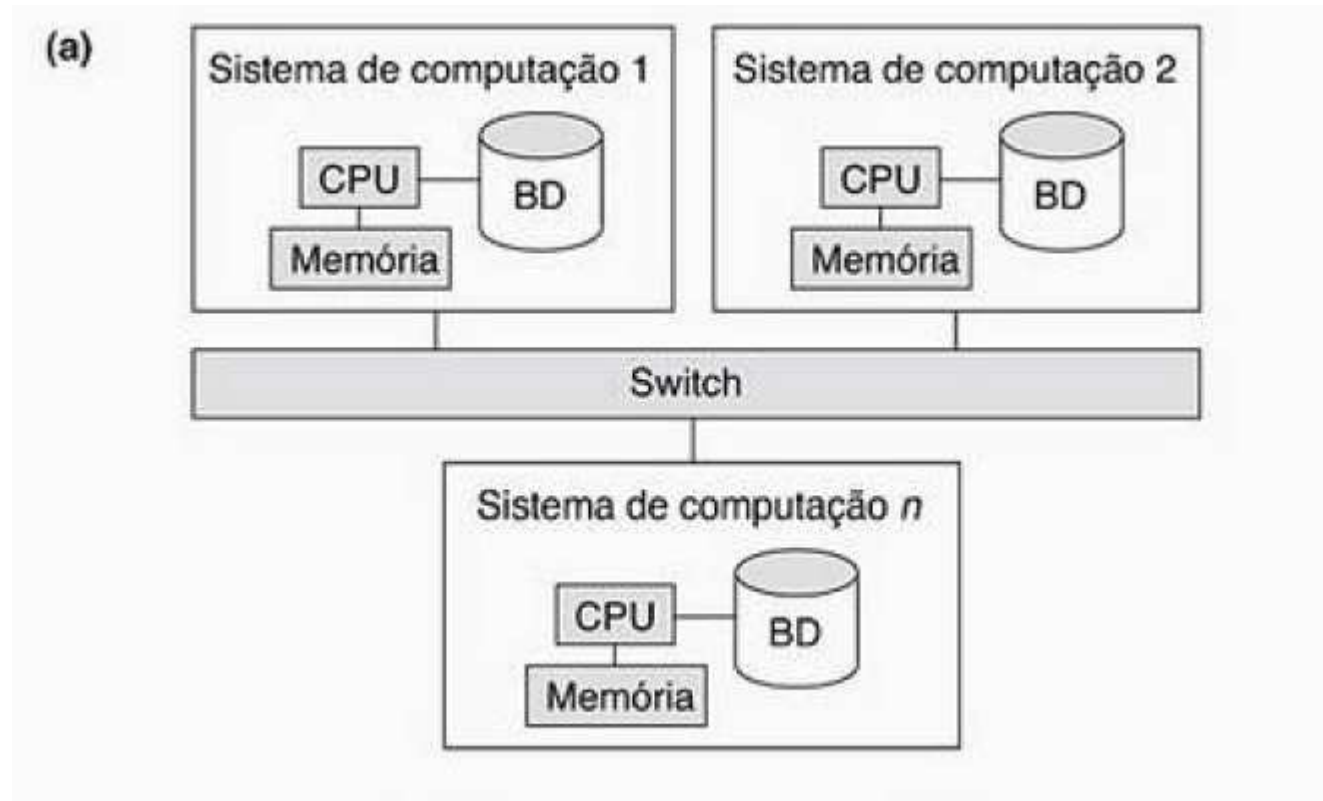
Arquitetura de sistemas servidor

- Servidores de transação
 - Também conhecidos como **servidores de consulta**
 - Clientes enviam **requisições** aos servidores que processam e devolvem o resultado
 - A mais utilizada!
- Servidores de dados
 - Usados em redes locais
 - Conexão de alta velocidade entra cliente-servidor
 - Tarefas exigem muita computação
 - Passa os **dados** para serem **processados no cliente** que tem um backend completo

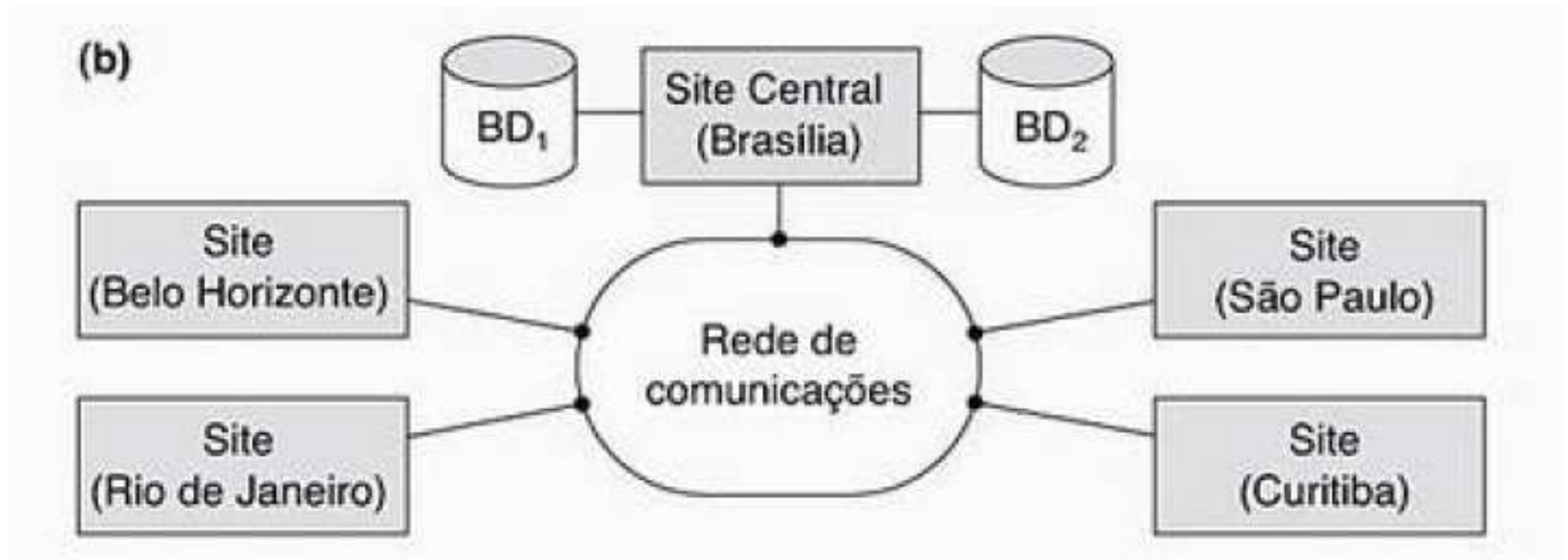
Arquiteturas paralelas x distribuídas.

- Arquitetura de sistemas multiprocessador (**paralela**)
 - Memória compartilhada (altamente acoplada)
 - Disco compartilhado (livremente acoplada)
 - Nada compartilhado
- Não tem overhead de mensagem por uma rede.
- Para essas arquiteturas usamos os sistemas de banco de dados paralelos.

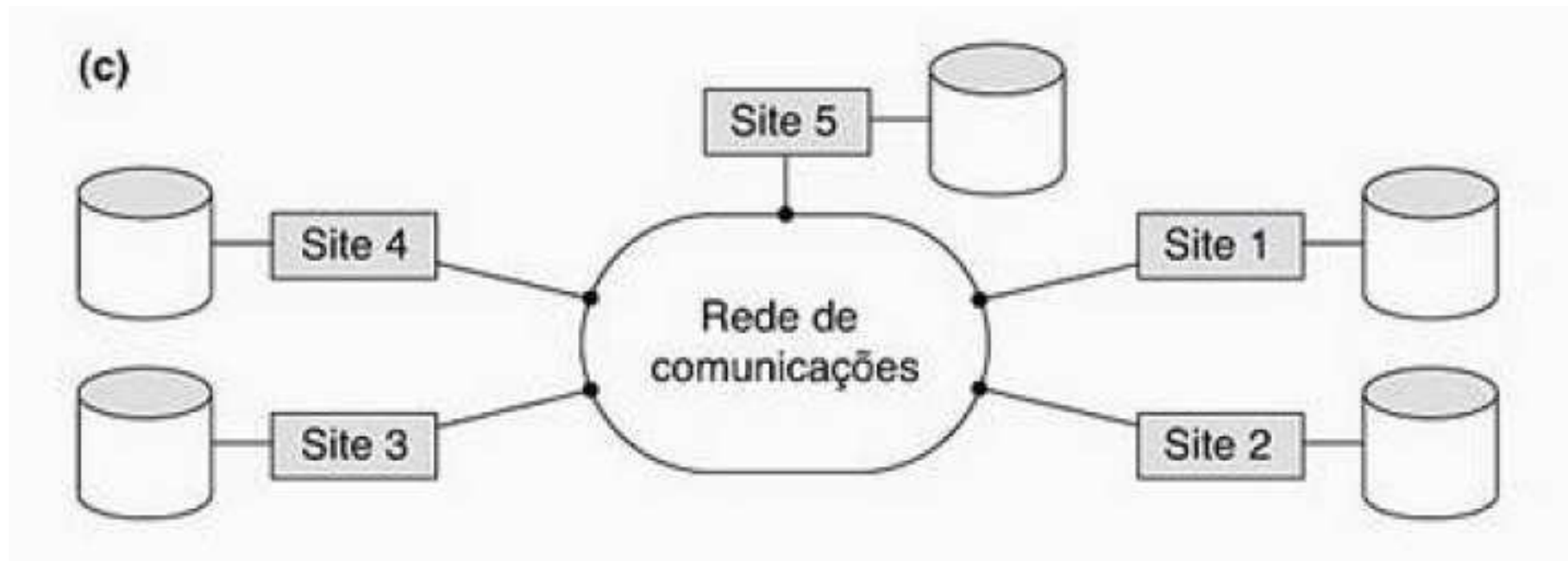
Banco de dados paralelo – Nada compartilhado



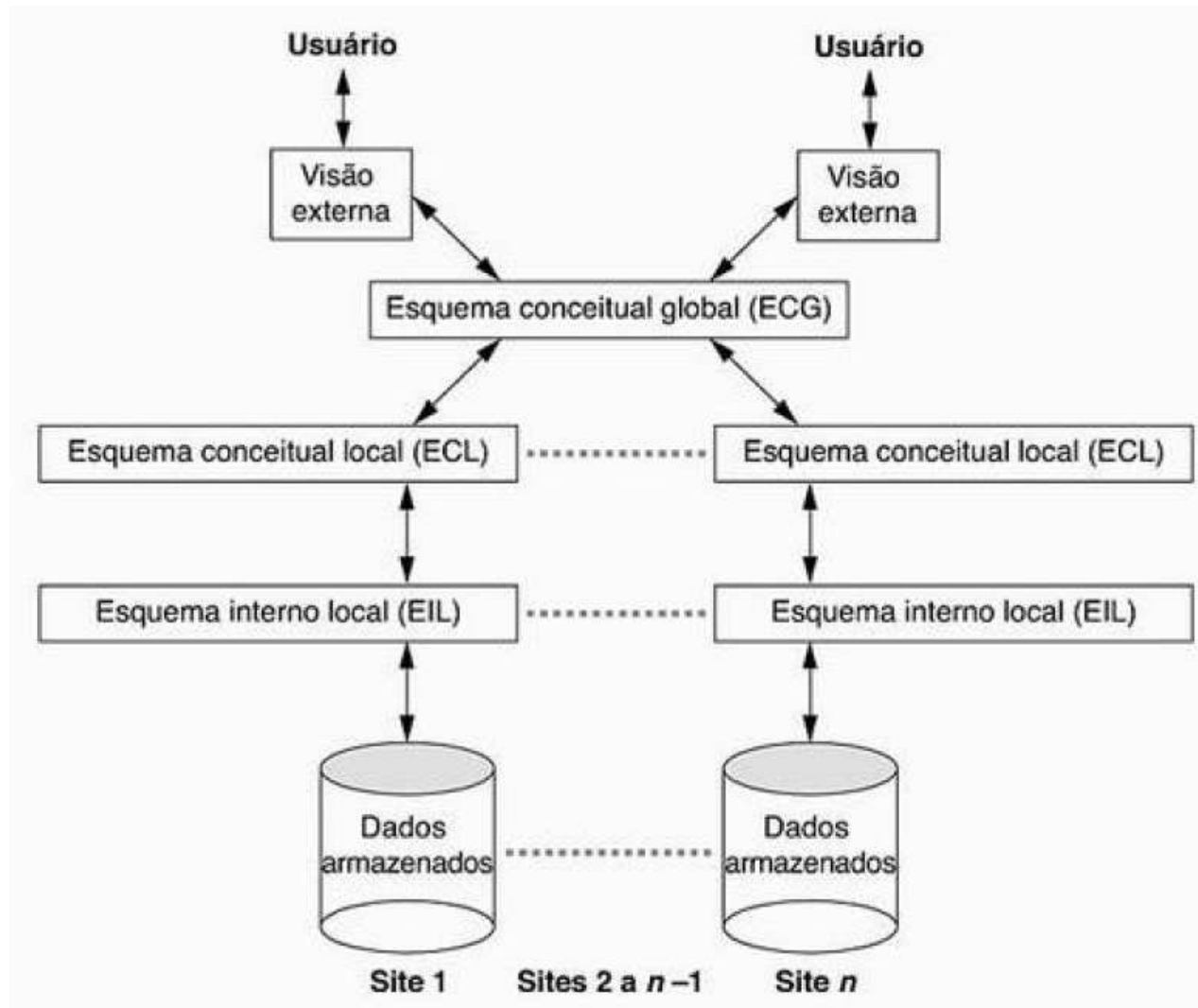
Banco de dados centralizado com acesso distribuído



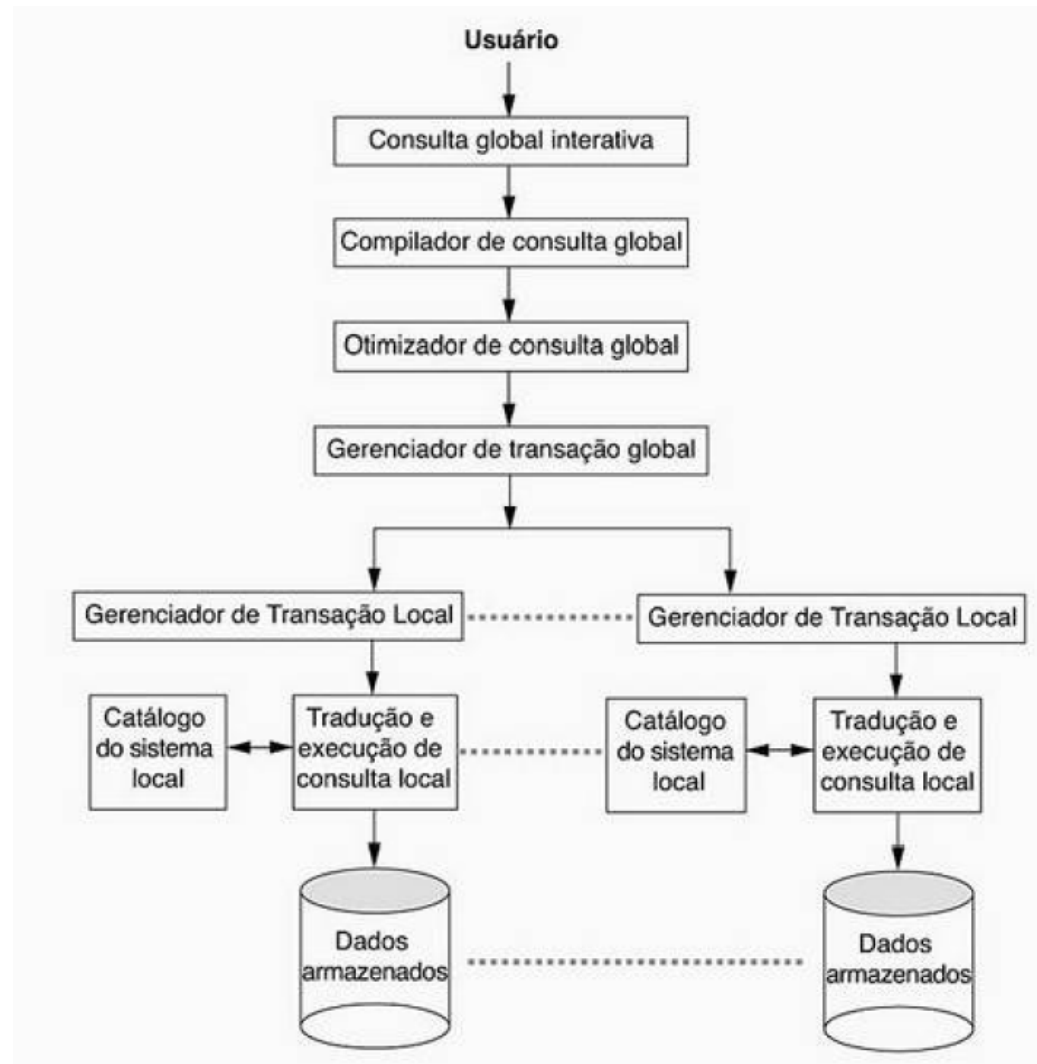
Banco de dados distribuído puro



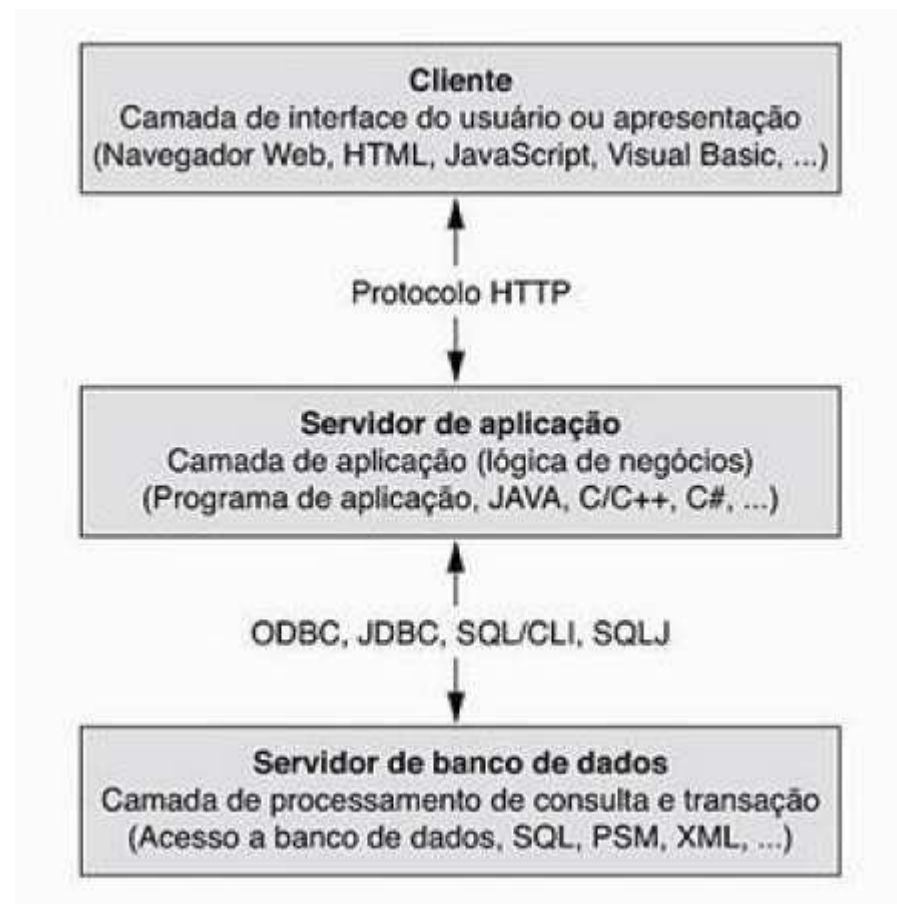
Arquitetura do esquema para BDDs



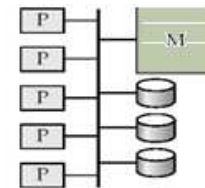
Arquitetura de componentes para BDDs



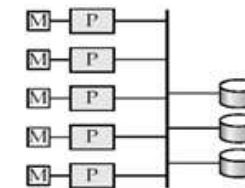
Arquitetura cliente servidor 3 camadas



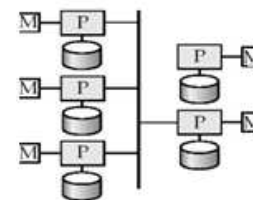
Banco de dados paralelo



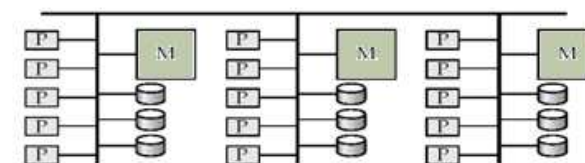
(a) shared memory



(b) shared disk



(c) shared nothing



(d) hierarchical

Conceito - Granularidade grossa x fina

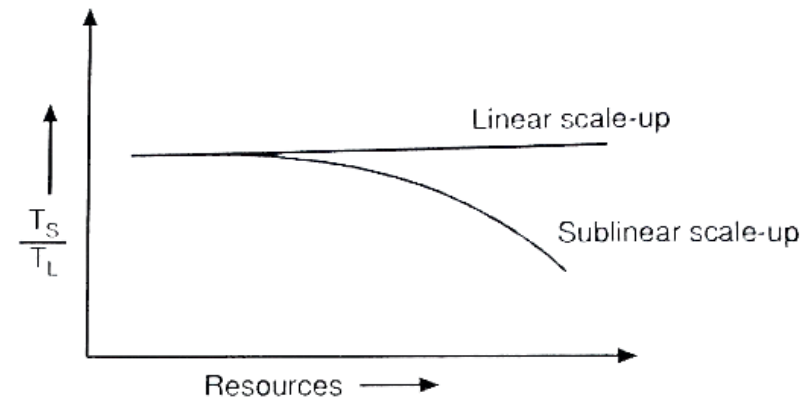
- Granularidade grossa
 - Consiste em poucos e poderosos processadores
- Granularidade fina
 - Usa milhares de pequenos processadores

Sistemas paralelos

- Muitas operações são realizadas em paralelo
- Melhoram as velocidades
 - De processamento
 - De Entrada e Saída (E/S)
 - Usando várias CPUs e discos em paralelo.
- Medidas de desempenho
 - **Throughput** – número de tarefas em determinado intervalo de tempo
 - **Tempo de resposta** – tempo para completar uma tarefa determinada

Ganho de velocidade e escala

- Ganho de velocidade
 - Linear ou sublinear



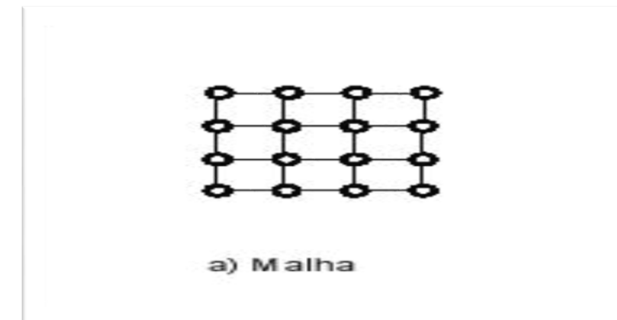
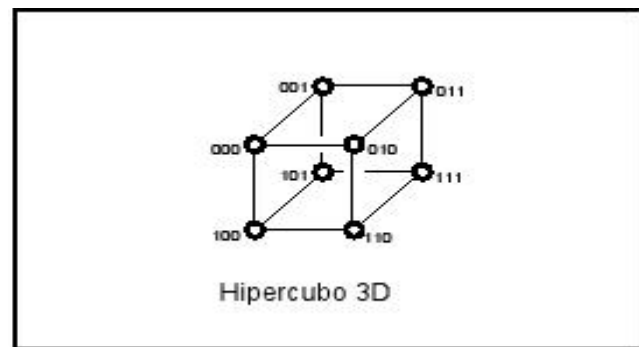
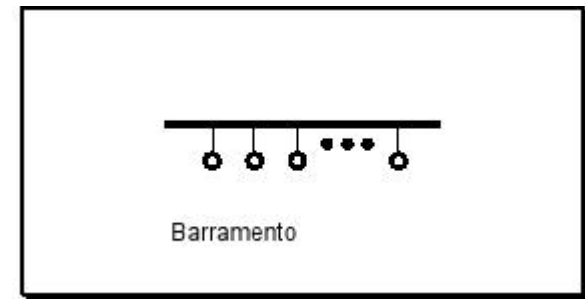
- Ganho de escala
 - Em batch ou de transação
 - **Métrica mais importante** para medir a eficiência em banco de dados paralelos

Fatores contrários ao paralelismo

- Custo de partida – associado ao início do processo
- Interferência – processo que acessam recursos compartilhados
- Distorções – Dividir uma tarefa em partes com igual tempo de processamento pode se complicado

Redes de interconexões

- Processador, disco e memória
 - Precisam de um rede de conexão
- Tipos de redes
 - Barramento
 - Malha
 - Hipercubo



Arquitetura paralelas de banco de dados

Memória compartilhada

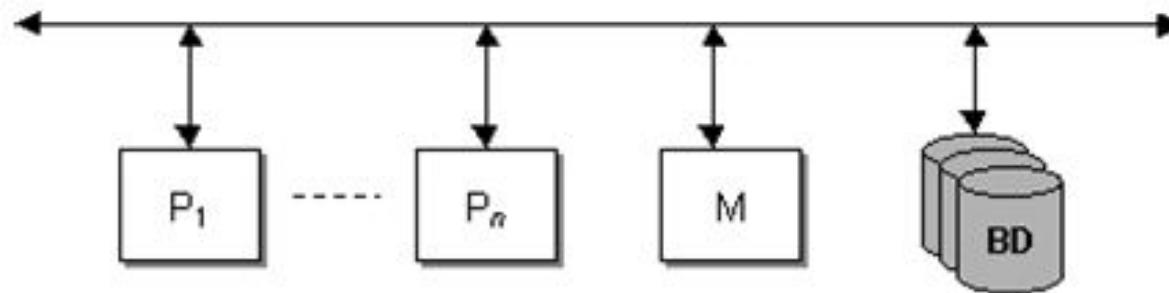
Disco compartilhado

Nada compartilhado

Hierárquico

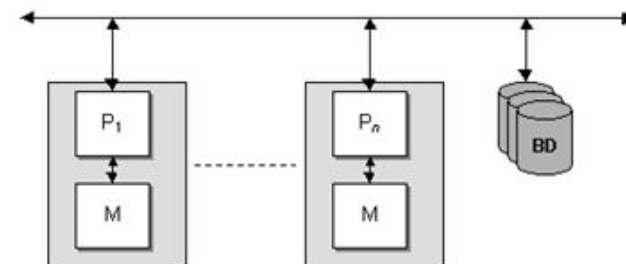
Memória compartilhada

- Todos os processadores compartilham a mesma memória
- Vantagens: extrema eficiência na comunicação entre processadores
- Desvantagens: a arquitetura não é adequada ao uso de mais de 32 ou 64 processadores



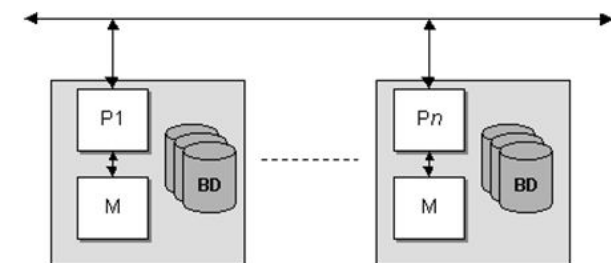
Disco compartilhado

- Todos os processadores compartilham um conjunto comum de discos
- Geralmente são chamados de clusters
- Vantagens:
 1. o acesso à memória não representa um gargalo;
 2. é um modo barato de aumentar a tolerância a falhas;
- Desvantagem: é novamente o grau de crescimento



Nada compartilhado

- Os processadores não compartilham nem a memória nem o disco
- Vantagem:
 - Toda requisição de E/S não passa pela rede
 - Suporte a um grande número de processadores
- Desvantagem:
 - Comunicação entre processadores é o fator limitante
 - Acesso ao disco não local



Hierárquico - Modelo híbrido

- Este modelo combina características de várias arquiteturas anteriores
- Reduz a necessidade e complexidade da comunicação entre processadores.

Paralelismos!

- Paralelismo de I/O
 - Reduzir o tempo de recuperação por meio do particionamento de uma relação em vários discos
 - Estratégias: Round-robin, P. Hash, por faixa.
- Paralelismo Interconsultas
 - Consultas ou transações diferentes são executadas em paralelo
- Paralelismo Intraconsultas
 - Dividir uma consulta entre diversos processadores e discos
 - Pode ser: intra-operação ou interoperação

Custos da Avaliação Paralela de Operações

- Custo de inicialização
 - Iniciar em diferentes processadores
- Desbalanceamento da distribuição de trabalho
 - Processadores recebendo mais tuplas que outros
- Retenção de recursos (memória, disco e rede)
 - Resultando em atrasos
- Custo de montagem do resultado final
 - Inclui a transmissão dos resultados parciais a partir de cada processador.

Questão 01 - CESPE - 2013 - SERPRO - Analista - Desenvolvimento de Sistemas

Acerca dos conceitos e aplicações de banco de dados distribuído, programação distribuída e processamento em GRID, julgue os seguintes itens

[112] O sistema de gerenciamento de banco de dados paralelo compartilha memória e(ou) disco, ao passo que o sistema de gerenciamento distribuído consiste em vários elementos de processamento conectados por meio de uma rede de comunicação.

Banco de dados distribuídos

Introdução



Conceito

- Sistema de computação distribuído
 - Uma série de elementos de processamento, não necessariamente homogêneos, que são interconectados por uma rede de computadores e que cooperam na realização de certas tarefas atribuídas.



Banco de dados distribuídos

- Uma coleção de múltiplos bancos de dados logicamente inter-relacionados, distribuídos por um rede de computadores, e um sistemas de banco de dados distribuídos (SGBDD)
 - **SGBDD** – um sistema que gerencia o BDD enquanto torna a distribuição transparente pra o usuário.



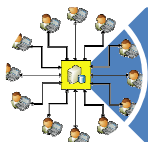
Uma princípio fundamental

Para o usuário, um sistema distribuído deve parecer exatamente como um sistema não distribuído

Regras associadas ou objetivos secundários



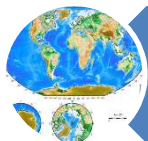
Autonomia local



Não dependência de um site central



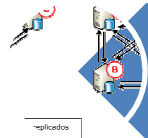
Operação contínua



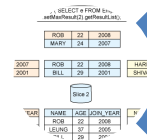
Independência de localização



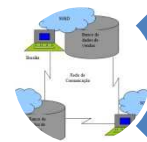
Independência de fragmentação



Independência de replicação



Processamento de consultas distribuído



Gerenciamento de transações distribuídas



Independência de Hardware



Independência de sistema operacional



Independência de rede



Independência de SGBD

Questão 02 - CESGRANRIO - 2008 - Órgão: Petrobras

Ana. de Sistemas Júnior - Processos de Negócios

Sistemas de informações distribuídos são aqueles em que dados são armazenados e processados em diferentes localizações. Um banco de dados distribuído é um exemplo deste tipo de sistema. Para o usuário, um sistema de banco de dados distribuído deve parecer exatamente como um sistema não distribuído. Para que tal meta seja alcançada, alguns objetivos secundários são normalmente estabelecidos, entre os quais NÃO se inclui a

- a) independência de localização.
- b) independência de fragmentação.
- c) independência do sistema operacional.
- d) operação contínua.
- e) coordenação em um nó central.

Diferenças entre Paralelo (multiprocessador) e Distribuído

- Condições para ser distribuído:
 1. Conexão dos nós de banco de dados por uma **rede de computadores**
 2. Inter-relação **lógica** dos bancos de dados conectados
 3. **Ausência** de restrição de **homogeneidade** entre os nós conectados

Questão 03 - CESPE - 2013 - SERPRO - Analista – Admin. de Serviços de Tecnologia da Informação

A respeito de banco de dados, julgue os itens subsequentes

[111] São características diferenciadoras dos bancos de dados distribuídos, em comparação com os bancos de dados paralelos, a distribuição física geográfica, a administração separada e a intercomunicação menor.

Transparência

- Transparência de organização dos dados
 - Local – o comando para executar uma tarefa independe do local dos dados e de onde o comando foi emitido.
 - Nomes – quando um nome é associado a um objeto, os objetos nomeados são acessados sem ambiguidade, sem especificação adicional sobre o local onde os dados se encontram.

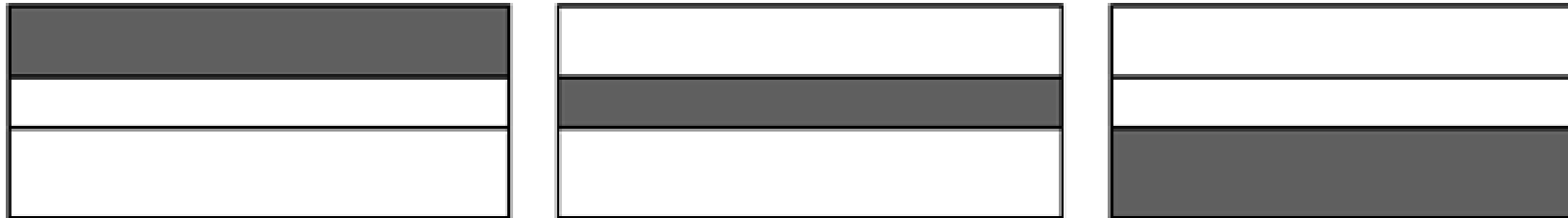
Transparência de replicação

- As cópias dos mesmos objetos podem estar armazenadas em vários sites
 - Melhora a disponibilidade, desempenho e confiabilidade
- Torna o usuário desavisado da existência dessas cópias

Transparência de fragmentação

- Fragmentação horizontal
 - Subconjunto das tuplas de uma tabela
 - Fragmentação vertical
 - Subconjunto das colunas de uma relação
 - Fragmentação mista
-
- Mesmo que uma consulta tenha que ser dividida em sub-consultas esse processo é transparente para o usuário.

Fragmentação



(a) Horizontal Fragmentation



(b) Vertical Fragmentation

Outras transparências

- Transparência de projeto
 - Liberdade de projeto
 - Como o banco de dados é projetado
- Transparência de execução
 - Onde a transação é executada



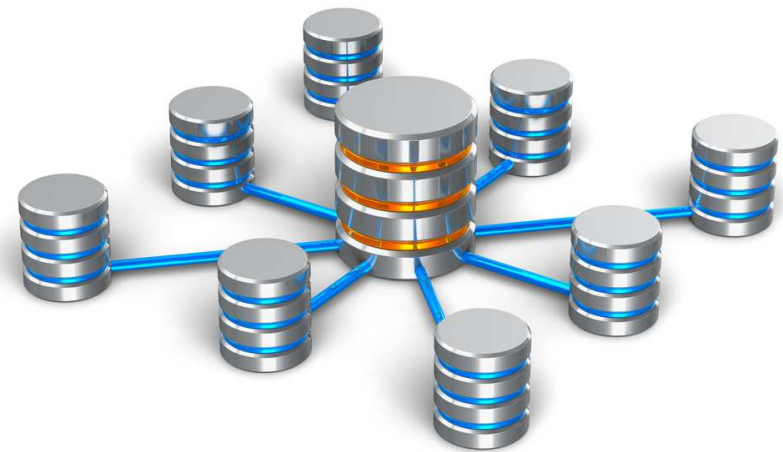
Autonomia

- Determina a extensão à qual os nós individuais ou BDs em um BDD conectado podem operar independentemente.
 - Projeto – modelo de dados e gerenciamento de transações
 - Comunicação – sobre o compartilhamento de informações com outros nós
 - Execução – atuação dos usuários conforme desejarem

Confiabilidade e disponibilidade

- São duas vantagens dos BDD:
 - Confiabilidade – a probabilidade do sistema estar funcionando em certo ponto do tempo (momento ou instante)
 - Disponibilidade – a probabilidade de que o sistema esteja continuamente disponível durante um intervalo de tempo (intervalo)

BDD: Vantagens, taxonomia, replicação e fragmentação



Vantagens dos BDs distribuídos

- Maior facilidade e flexibilidade no desenvolvimento de aplicações
 - Consequência da transparência de distribuição
- Maior confiabilidade e disponibilidade
 - Isolamento de falhas ao site de origem
 - Replicação de dados e software
- Maior desempenho
 - Fragmentação
 - Paralelismo

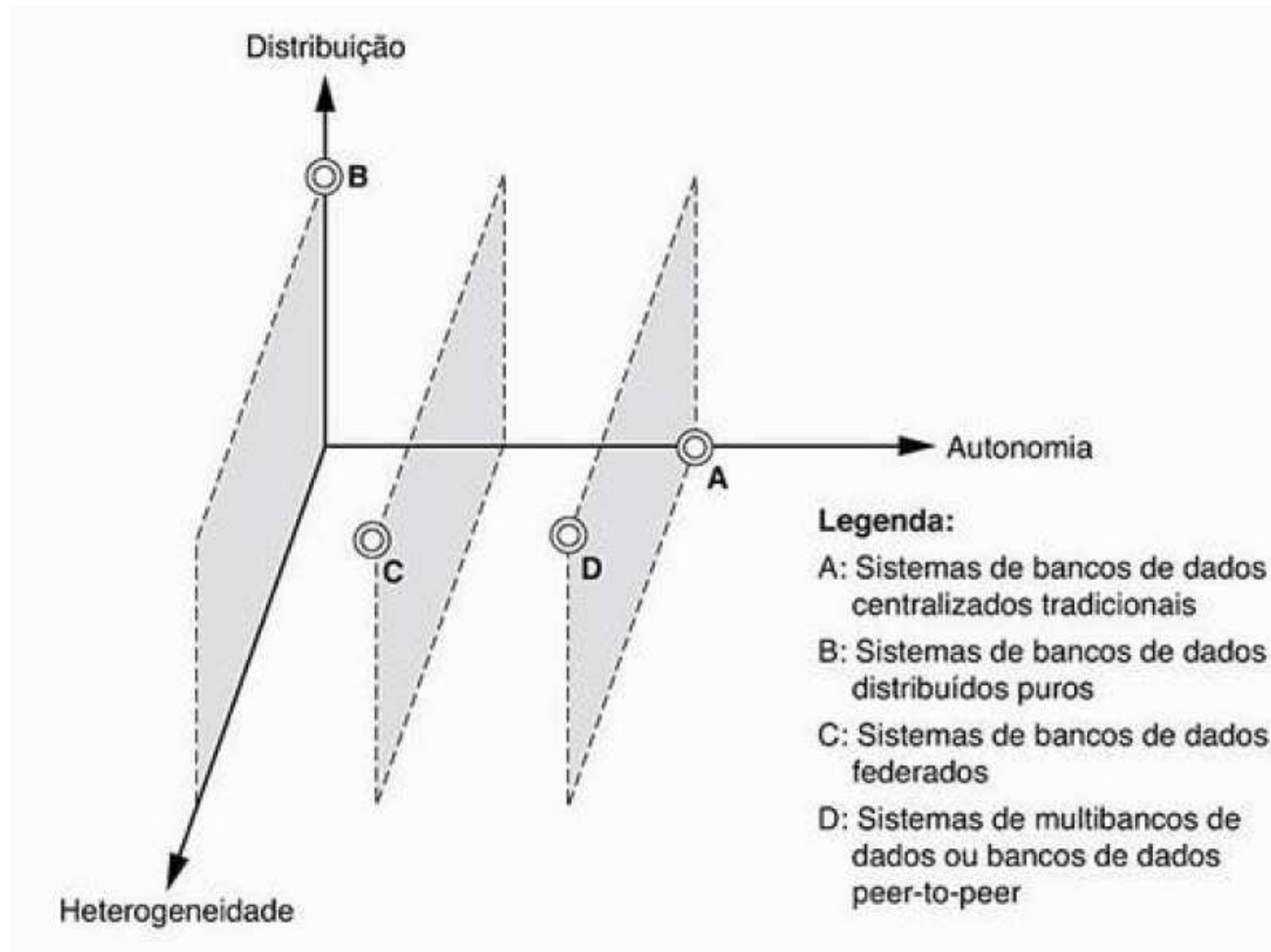
Vantagem dos BDs distribuídos

- Expansão mais fácil
 - Aumento da quantidade de dados
 - Aumento do tamanho do banco de dados
 - Aumento do número de processadores

Tipos de SBDD (taxonomia)

- Grau de homogeneidade
 - Homogêneo ou heterogêneo
- Grau de autonomia local
 - Sem ou com autonomia
- Grau de distribuição
 - Centralizado ou distribuído

Classificação dos SBDD



Questão 04 - CESPE - 2013 - Órgão: INPI -Analista de Planejamento - Des. e Manutenção de Sistemas

Em relação a Data Warehouse, Data Mining e banco de dados distribuídos, julgue os itens subsequentes.

[1] Como meta genérica, um sistema gerenciador de banco de dados distribuído (SGBDD) processa grandes volumes de dados, dividindo-os e processando-os em partes menores, de maneira coordenada, o que possibilita que cada parte do processamento seja autônoma. Nos casos em que todas as partes de software e hardware do SGBDD sejam iguais e todos os usuários (clientes) utilizem um software idêntico, esse tipo de SGBDD é chamado federado.

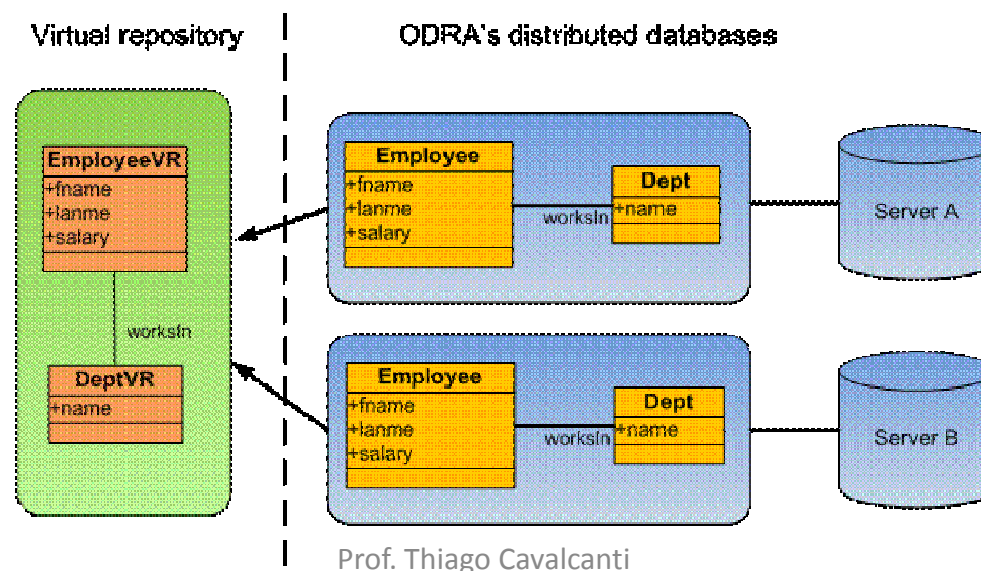
Sistemas de BD federados (Problemas)

- Heterogeneidades:
 - Modelos de dados
 - Restrições
 - Linguagem de consulta
 - Semântica – ocorre quando existem diferenças no significado, interpretação e uso intencionado dos mesmos dados ou dados relacionados
 - Problemas: Universo do discurso, representação e nomeação, subjetividade dos dados, restrição de transações ...

Funções adicionais dos BDDs

- Acompanhar a distribuição de dados
- Processamento de consulta distribuído
- Gerenciamento de transações distribuídas
- Gerenciamento de dados replicados
- Recuperação de banco de dados distribuídos
- Segurança
- Gerenciamento de diretório ou catálogo de dados distribuídos

Fragmentação e Replicação



Fragmentação de dados

- A informação sobre a fragmentação, replicação e alocação de dados é armazenada no diretório global.
- Fragmentação horizontal
 - Subconjunto de tuplas de uma relação
 - Ex. Um site para cada departamento
- Fragmentação vertical
 - Divide a relação verticalmente por colunas
 - Cada fragmento mantém apenas certos atributos
 - Ex: Informações pessoais e de trabalho de um FUNC

Questão 05 - Banca: FCC - 2012 - Órgão: TST - Prova: Analista Judiciário - Tecnologia da Informação

Uma das formas de implementação de um banco de dados ocorre por meio da distribuição de dados em mais de um local. Essa distribuição pode ser feita por meio da chamada fragmentação vertical, na qual

- a) os índices são divididos em dois índices, sendo que há um índice principal e um outro secundário.
- b) o arquivo de log do banco de dados sofre um processo de criptografia e armazenamento redundante.
- c) as tabelas do banco de dados são decompostas, ou seja, os atributos das tabelas são divididos nos diversos locais.
- d) parte dos dados do banco de dados são convertidos para o formato XML.
- e) é armazenada exatamente uma tabela do banco de dados original em cada local.

Replicação e alocação de dados

- BDD Totalmente replicado
 - Melhora a disponibilidade e **desempenho de recuperação**
 - **Desvantagem:** Operações de atualização!
- **Alocação não redundante**
- Replicação parcial
 - Comum em profissionais de vendas
- Esquema de replicação
 - Descreve a replicação dos fragmentos.
 - Distribuição de dados

Exemplo

FUNC_DEP_5

Pnome	Minicial	Unome	Cpf	Salario	Cpf_supervisor	Dnr
João	B	Silva	12345678966	30.000	33344555587	5
Fernando	T	Wong	33344555587	40.000	88866555576	5
Ronaldo	K	Lima	66688444476	38.000	33344555587	5
Joice	A	Leite	45345345376	25.000	33344555587	5

DEP_5

Dnome	Dnumero	Cpf_gerente	Data_inicio_ger
Pesquisa	5	33344555587	22-05-1988

LOCAL_DEP_5

Dnumero	Localizacao
5	Santo André
5	Itu
5	São Paulo

TRABALHA_EM_DEP_5

Ecpf	Pnr	Horas
12345678966	1	32,5
12345678966	2	7,5
66688444476	3	40,0
45345345376	1	20,0
45345345376	2	20,0
33344555587	2	10,0
33344555587	3	10,0
33344555587	10	10,0
33344555587	20	10,0

PROJ_DEP_5

Projnome	Projnumero	Projlocal	Dnum
ProdutoX	1	Santo André	5
ProdutoY	2	Itu	5
ProdutoZ	3	São Paulo	5

Dados no site 2

FUNC_DEP_4

Pnome	Minicial	Unome	Cpf	Salario	Cpf_supervisor	Dnr
Alice	J	Zelaya	99988777767	25.000	98765432168	4
Jennifer	S	Souza	98765432168	43.000	88866555576	4
André	V	Pereira	98798798733	25.000	98765432168	4

DEP_4

Dnome	Dnumero	Cpf_gerente	Data_inicio_ger
Administração	4	98765432168	01-01-1995

LOCAL_DEP_4

Dnumero	Localizacao
4	Mauá

TRABALHA_EM_DEP_4

Ecpf	Pnr	Horas
33344555587	10	10,0
99988777767	30	30,0
99988777767	10	10,0
98798798733	10	35,0
98798798733	30	5,0
98765432168	30	20,0
98765432168	20	15,0

PROJ_DEP_4

Projnome	Projnumero	Projlocal	Dnum
Informatização	10	Mauá	4
Novos_beneficios	30	Mauá	4

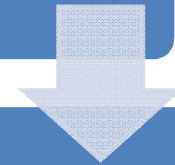
Dados no site 3

Processamento e otimização de consulta

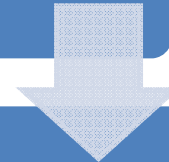


Processamento e otimização de consulta

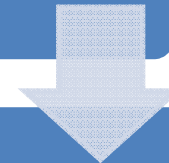
Mapeamento da consulta



Localização



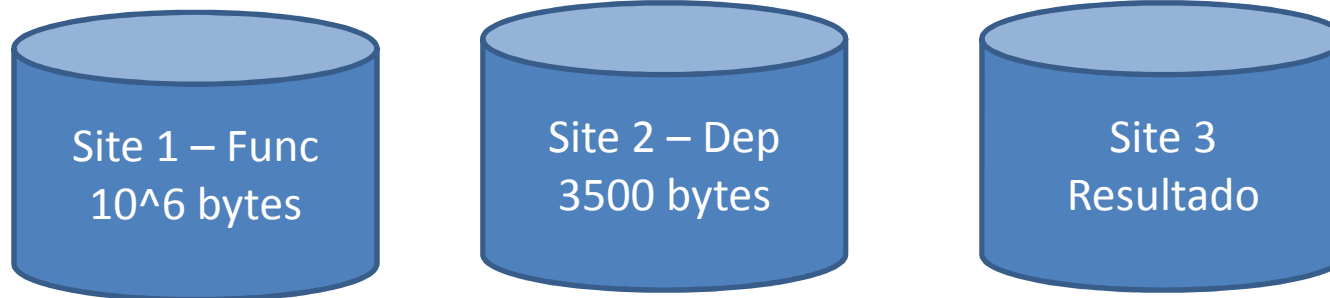
Otimização global da consulta



Otimização local da consulta

Custo para transferência de dados no processamento

- Transferir dados pela rede
 - Quanto custa?
 - Arquivos intermediários ou finais?
 - Qual a rede comunica os sites ou sistemas?



Dados das tabelas funcionário e departamento

Site 1:

FUNCIONARIO

Pnome	Minicial	Unome	Cpf	Datanasc	Endereco	Sexo	Salario	Cpf_supervisor	Dnr
-------	----------	-------	-----	----------	----------	------	---------	----------------	-----

10.000 registros

cada registro tem 100 bytes

Campo Cpf tem 11 bytes

Campo Pnome tem 15 bytes

Campo Dnr tem 4 bytes

Campo Unome tem 15 bytes

Site 2:

DEPARTAMENTO

Dnome	Dnumero	Cpf_gerente	Data_inicio_ger
-------	---------	-------------	-----------------

100 registros

cada registro tem 35 bytes

Campo Dnumero tem 4 bytes

Campo Dnome tem 10 bytes

Campo Cpf_ger tem 11 bytes

Utilizando semi-junção

- Operação de semi-junção
 - Reduzir o número de tuplas de uma relação antes de transferi-la para outro site.
 - Apenas o atributo de junção é transferida num primeiro momento
- Se apenas um conjunto pequeno de tuplas participar da junção, essa é a estratégia mais eficiente.
- Decomposição de consulta
 - Transparência de distribuição

Visão geral do gerenciamento de transações

Primitive	Description
BEGIN_TRANSACTION	Mark the start of a transaction
END_TRANSACTION	Terminate the transaction and try to commit
ABORT_TRANSACTION	Kill the transaction and restore the old values
READ	Read data from a file, a table, or otherwise
WRITE	Write data to a file, a table, or otherwise

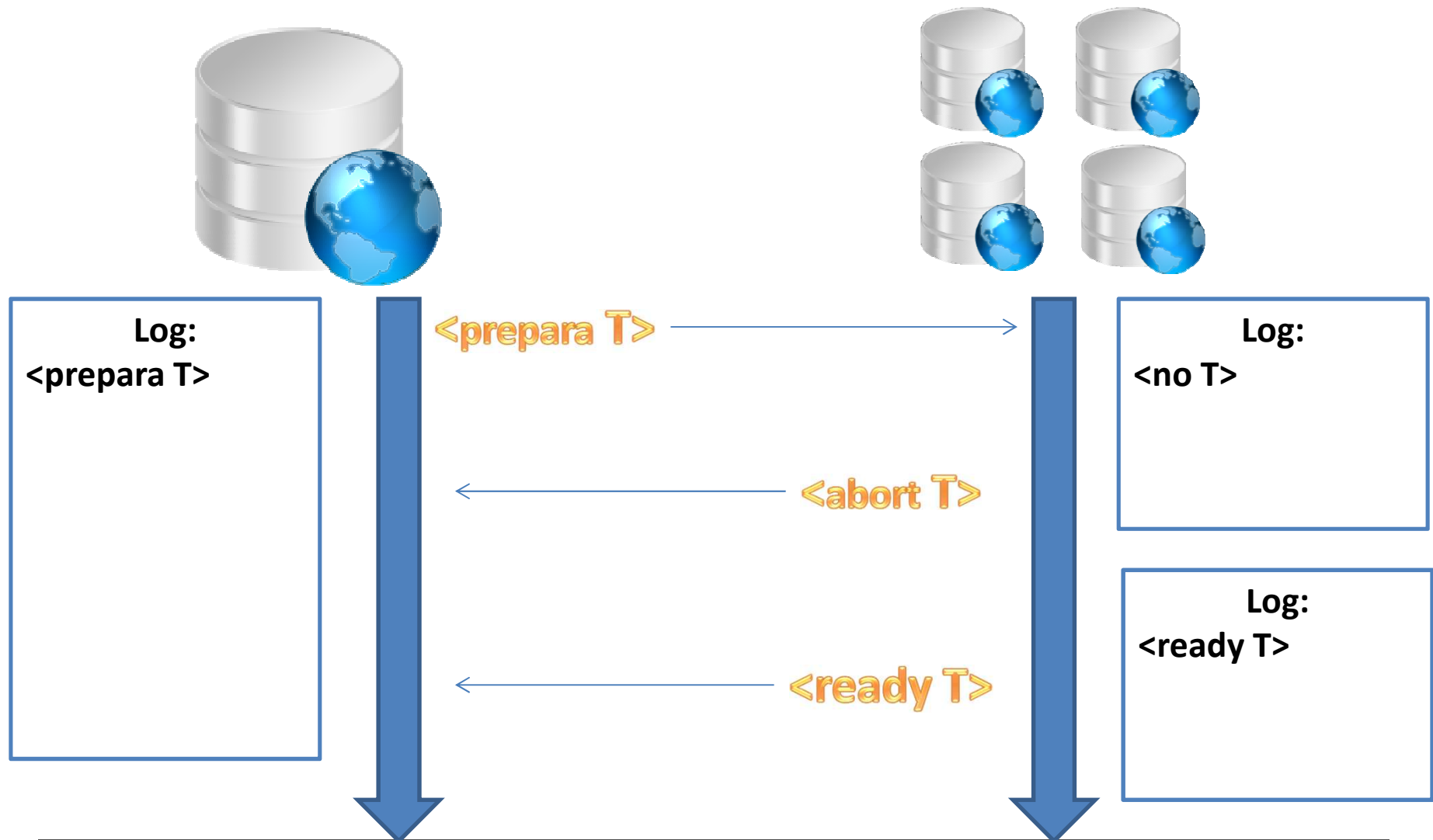
Protocolo de Efetivação em BDD

- Se desejarmos garantir a atomicidade, todos os sites envolvidos na execução de uma transação T devem concordar com o seu término:
 - Protocolo de efetivação em duas fases
 - Protocolo de efetivação em três fases
- A partir de agora quando falarmos de S1 e C1 estaremos nos referindo a **Site** e **Coordenador**

Commit Protocol em duas fases

- Fase 01
 - C1 - Acrescenta o registro <**prepare** T> no log e força a manutenção do log em memória estável
 - C1 - Envia a mensagem **prepare** T para todos os sites em que T é executada.
 - S1 – Ao receber a mensagem, o gerenciador de transações do site determina se é possível efetivar sua porção da transação T
 - S1 – Se a resposta for negativa, ele adicionará um registro <no T> no log e enviará uma mensagem de **abort** T para C1
 - S1 – Se a resposta for positiva, ele adicionará um registro de <**ready** T> para o log e importará o log (com todos os registros de T) à memória estável e enviará uma mensagem de **ready** T para C1

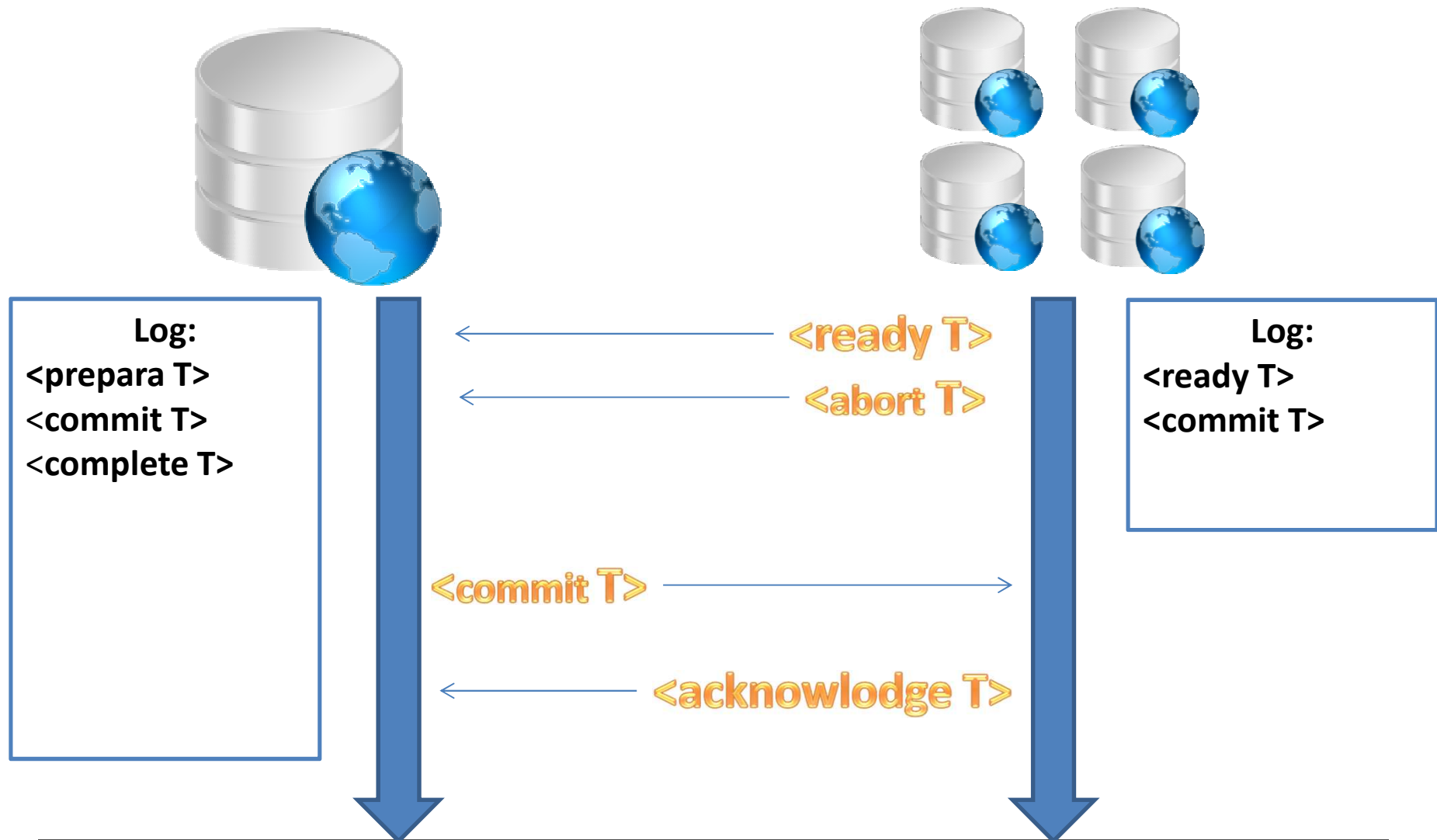
Commit Protocol em duas fases (Fase 1)



Commit Protocol em duas fases

- Fase 02
 - C1 – recebe de todos os sites mensagens de resposta ao **prepare T** ou é completado um intervalo de tempo prefixado.
 - Baseado nessas informações ele determina se a transação deve ser:
 - Efetivada – se C1 receber uma mensagem **ready T** de todos os sites participantes.
 - Será acrescentado um registro <**commit T**>
 - Abortado – se C1 receber pelo menos 1 mensagem de **abort T** de um dos sites participantes.
 - Será acrescentado um registro <**abort T**>
 - C1 – Mandará uma mensagem de commit ou abort a todos os sites participantes.

Commit Protocol em duas fases (Fase 2)



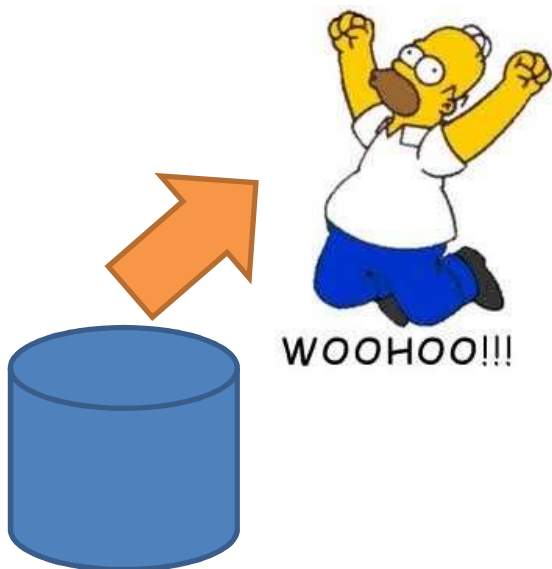
Manuseio de falhas

- Falha de um site participante
 - Ações do coordenador
 - Ações do Site após o retorno
 - Registros do log: commit, abort, ready, nada
- Falha no coordenador
 - Ações dos Sites
 - Ações do coordenador após o retorno
- Particionamento da rede

A maior desvantagem do protocolo 2PC é que uma falha do coordenador pode acabar em obstrução, que implica postergar a decisão de efetivar ou abortar T até que o coordenador volte a funcionar

Recuperação e Controle de Concorrência do 2PC

Volta de S



$T \rightarrow$ In-doubt



`<ready T> ? <commit T> ||
<abort T>`

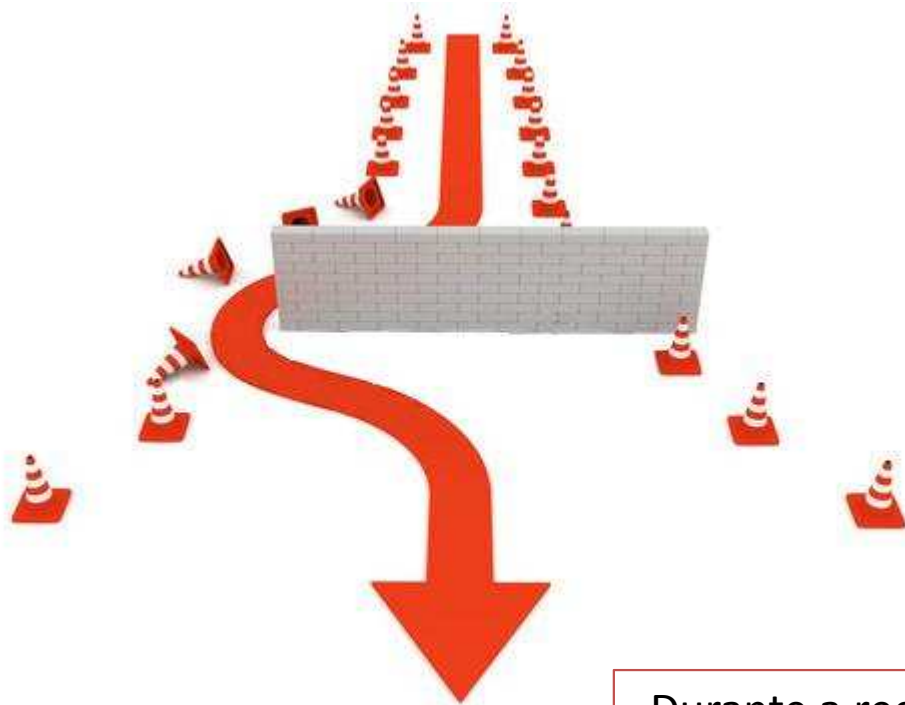
Volta a
processar!!



Recuperação e Controle de Concorrência do 2PC

- Descobrir o status das transações em dúvida pode ser demorado, pode ser necessário contatar diversos sites.
- Se o coordenador está fora do ar e nenhum outro site possui o status de uma transação incompleta, a recuperação fica **potencialmente obstruída caso se esteja usando o protocolo 2PC.**
 - Longo período ocioso!!!

Solucionado o problema

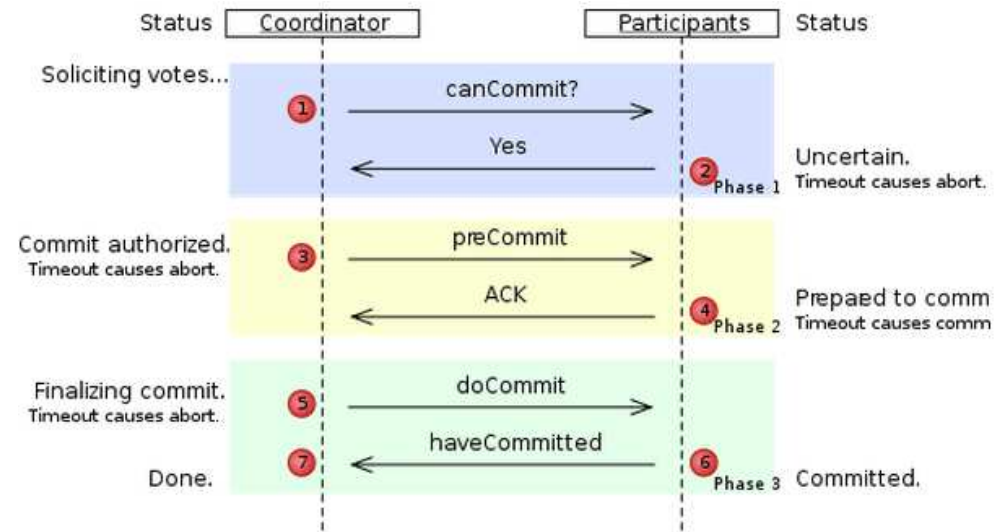


$\langle \text{ready } T \rangle \rightarrow$
 $\langle \text{ready } T, L \rangle$

L é a lista de todos os bloqueios realizados pela transação T

Durante a recuperação, depois das ações locais de recuperação, para toda transação com dúvida, todos os bloqueios notificados (L) são reassumidos.

Commit protocol em três fases



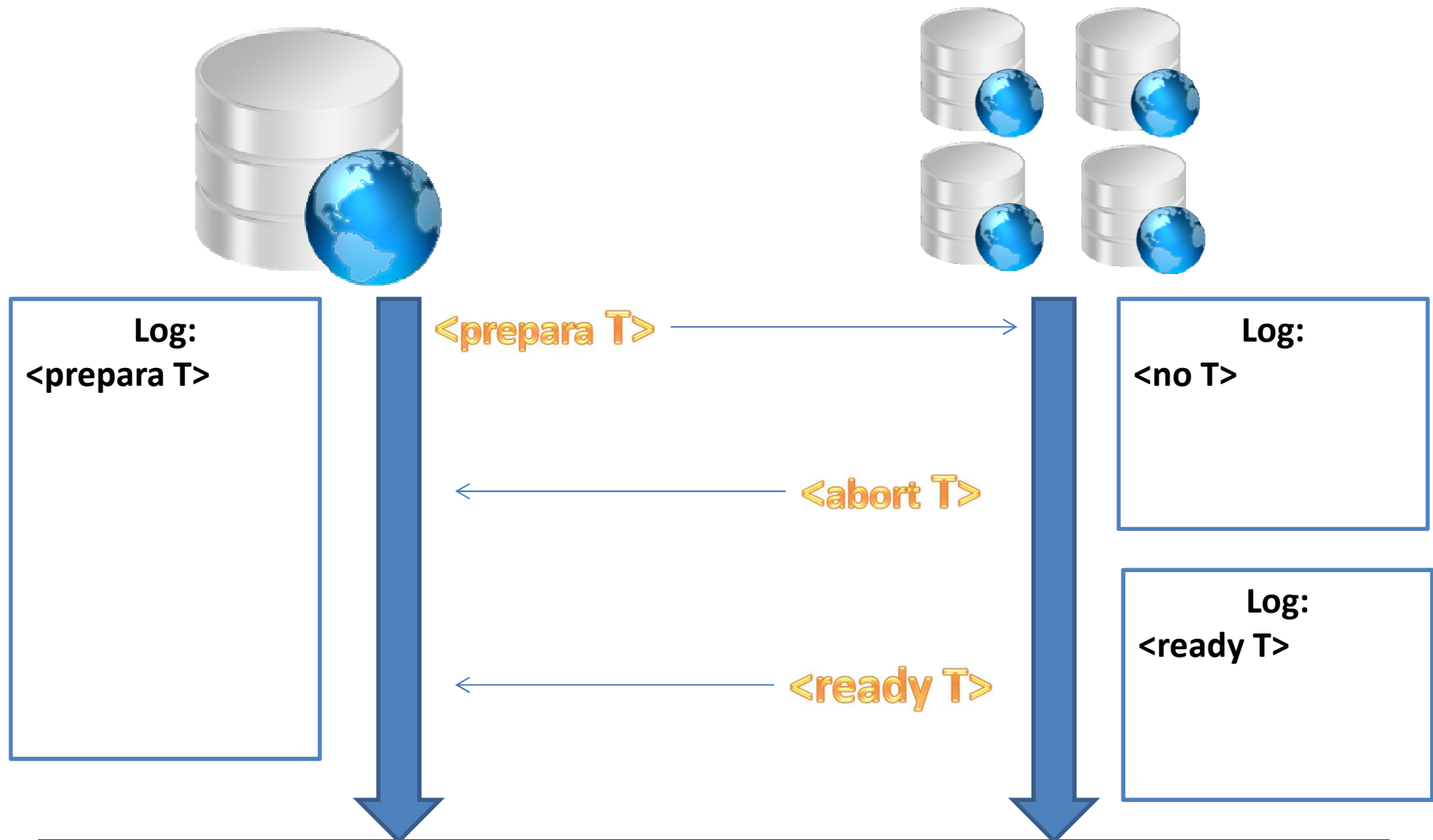
Commit protocol em três fases

- Premissas
 - Não ocorra particionamento de rede
 - No máximo K participantes **por transação** podem falhar enquanto o protocolo estiver sendo executado. K é um parâmetro indicativo da tolerância a falhas do protocolo nos sites
 - Em um tempo qualquer, ao menos $K + 1$ sites precisam estar ativos.

Commit protocol em três fases

- Fase 1. Idêntica a fase 1 do protocolo 2PC
- Fase 2.
 - C1 – Se não receber respostas de um site participante ou receber um **abort T**, então optará pelo **abort T**
 - C1 – Se recebe um **ready T** de todos os sites
 - LOG: *<precommit T>* - ainda pode ser abortada!
 - MSG: precommit T
 - S1 – Recebe o **precommit T**
 - LOG: *<precommit T>*
 - MSG: acknowledge T

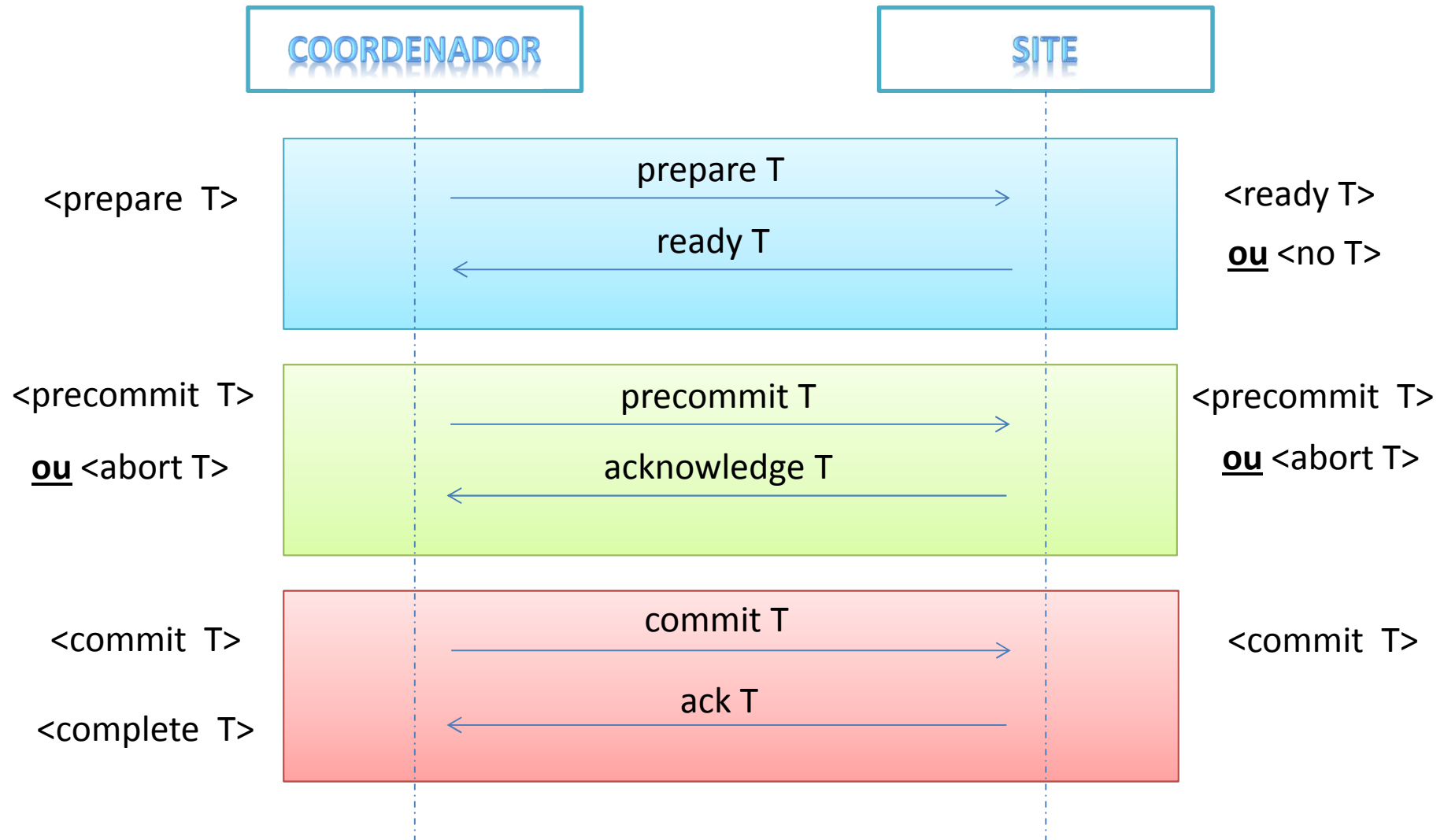
Commit Protocol em três fases (Fase 1)



Commit protocol em três fases

- Fase 3.
 - Esta fase é executada somente se na fase 2 for tomada a decisão de pré-efetivação
 - C1 – aguarda pelo menos K mensagens acknowledge
 - Toma a decisão em prol da efetivação
 - LOG: <commit T>
 - MSG: <commit T> a todos os sites participantes
 - S1 – recebe a mensagem
 - LOG: <commit T>

Commit em três fases



Questão 06 - CESGRANRIO - 2007 - Órgão: TCE-RO

Prova: Analista de Sistemas

No âmbito de bancos de dados distribuídos, o protocolo de efetivação 3PC (three-phase commit) exige que:

- I - não ocorra nenhum particionamento da rede;
- II - no máximo K participantes falhem enquanto o protocolo 3PC estiver sendo executado por transação;
- III - em um momento qualquer, pelo menos K+1 sites estejam ativos.

Considerando K um parâmetro indicativo da tolerância a falhas do protocolo nos sites, está(ão) correta(s) a(s) afirmativa(s):

- a) I, somente.
- b) II, somente.
- c) I e II, somente.
- d) II e III, somente.
- e) I, II e III.

Manuseio de falhas

- Falha em um site participante
 - Depende do que está escrito no log
- Falha no coordenador
 - Como não consideramos particionamento de rede a única falha possível é no coordenador.

Protocolo de Falha do Coordenador

- O protocolo de falha do coordenador é ativado por um site participante à medida que não recebe nenhuma resposta dentro de determinado intervalo de tempo.
 1. Os sites participantes **elegem um novo coordenador** usando um protocolo de eleição
 2. O novo coordenador, Cnovo, manda uma mensagem para cada site participante, solicitando o status local de T.
 3. Cada site participante. Inclusive Cnovo, determina o status local de T*
 4. Dependendo da resposta recebida, Cnovo decide se efetiva ou aborta T, ou se reinicia o protocolo 3 PC

Questão 07 - CESPE- 2008 - Órgão: STF Prova: Analista Judiciário - Tecnologia da Informação

O armazenamento e a recuperação de grandes quantidades de dados é um trabalho importante e muito explorado em um sistema gerenciador de banco de dados (SGBD). Com relação aos conceitos que envolvem esse sistema, julgue os itens que se seguem.

[1] O protocolo de falha do coordenador é executado em um sistema de banco de dados distribuídos quando um nó participante do sistema, por alguma razão, não recebe uma resposta do coordenador do sistema por determinado período de tempo.

Suporte de SO ao gerenciamento de transações

- Semáforos
 - Utilizar os recursos do sistema operacional para estruturar os bloqueios.
- Suporte especializado de hardware para bloqueio
- Fornecer um conjunto de operações básicas por meio de kernel.

Problemas presentes em SGBDDs

- Lidar com múltiplas cópias dos itens de dados
- Falha em sites individuais
- Falha em links de comunicação
- Confirmação distribuída
- Deadlock distribuído

Comentários sobre controle de concorrência

- Cópia distinguida
 - Bloqueio para esse item de dados são associados a ela, mas como escolher o site?
 - Técnica de Site primário
 - Site primário com Site de backup
 - Site primário com cópia primária
 - Quem possui a cópia deve atuar como coordenador.
- Controle de do concorrência baseado em votação

Comentários sobre recuperação distribuída

- Como determinar que um site está parado?
- O que acontece com uma mensagem enviada de um site para outro?
 - Como descobrir se o site recebeu ou não a mensagem?
- Usa-se o 2PC ou 3PC!

Questão 08 - CESPE - 2008 - Órgão: STF - Prova: Analista Judiciário - Tecnologia da Informação

O armazenamento e a recuperação de grandes quantidades de dados é um trabalho importante e muito explorado em um sistema gerenciador de banco de dados (SGBD). Com relação aos conceitos que envolvem esse sistema, julgue os itens que se seguem.

[1] Um dos problemas inerentes a uma arquitetura distribuída de banco de dados é o problema de tolerância a falhas, causado pelo fato de os dados estarem distribuídos entre os nós pertencentes ao banco distribuído. Entretanto, esse problema é resolvido mantendo-se uma cópia de cada dado pertencente ao banco em um único nó, conhecido como coordenador.

Gerenciamento do catálogo

- Crítico para garantir desempenho satisfatório
 - Autonomia dos sites
 - Gerenciamento de visões
 - Distribuição e Replicação
- Podemos ter catálogos:
 - Centralizados
 - Totalmente replicados
 - Particionados

Tendências atuais em BDD

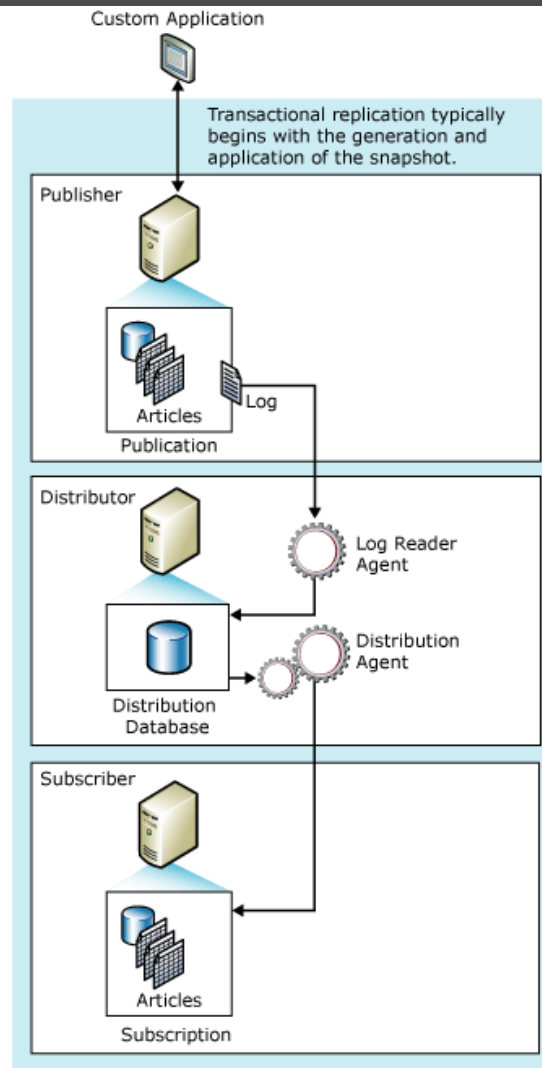
- Computação na nuvem
 - Paradigma que oferece infraestrutura de computação, plataformas e software como serviços pela internet
- Banco de dados Peer-to-peer (P2P)
 - Visa integrar as vantagens da computação P2P, como escalabilidade, resiliência a ataques e auto-organização, com recursos de gerenciamento de dados descentralizados.

Questão 09 - CESPE - 2012 - Órgão: MPE-PI - Prova: Analista Ministerial - Informática

A respeito de administração de banco de dados relacionais; administração de usuários e perfis de acesso; controle de proteção, integridade e concorrência; restauração de dados; tolerância a falhas e continuidade de operação e otimização de desempenho, julgue os itens de 85 a 87.

[86] Em sistemas distribuídos que utilizam técnicas de prevenção de impasses, o fato de um gráfico de espera ser acíclico indica a ausência de impasse, mesmo que a união dos gráficos locais gerem um gráfico global cíclico.

Transacional replication em SQL Server



Questão 10 - CESPE - 2013 - Órgão: TRT - 10ª REGIÃO (DF e TO) - Analista Judiciário – Tec. da Informação

Com relação a sistemas de gerenciamento de banco de dados, julgue os itens seguintes.

[1] Uma forma de se empregar o SQL para o gerenciamento de bancos de dados distribuídos é por meio de replicações transacionais, em que, na transactional publication, os dados são enviados apenas para os assinantes, e, na transactional publication with updatable subscriptions, as alterações são feitas tanto nas tabelas como nos assinantes.

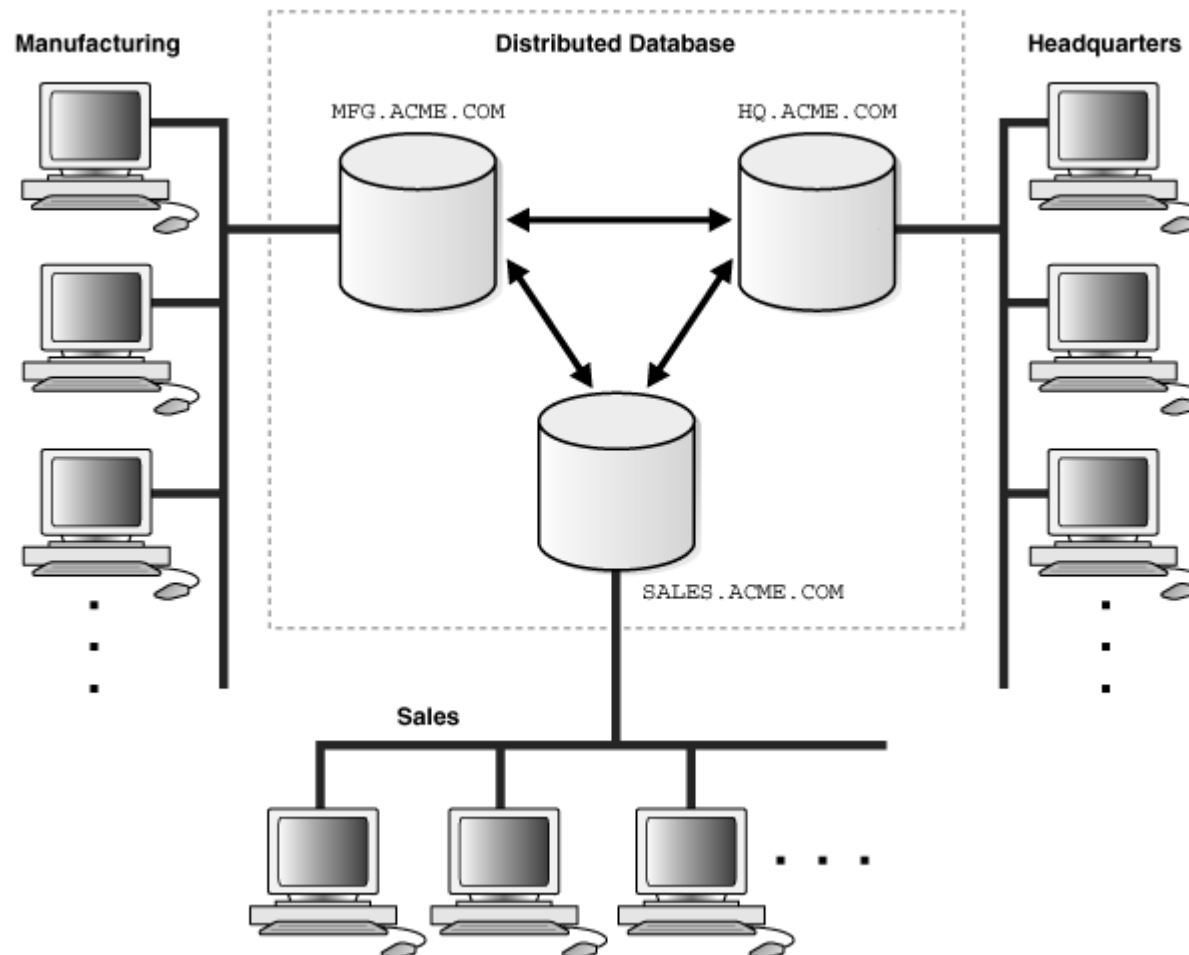
Banco de dados distribuídos Oracle



Banco de dados distribuídos Oracle

- Fornece suporte a arquitetura homogêneas, heterogêneas e cliente servidor.
- Utiliza o protocolo de efetivação em duas fases(2PC)
 - O processo RECO roda em segundo plano
- DBA pode reverter manualmente as transações em dúvida e liberar os recursos
- Oracle Net Services
 - Protocolo de redes padrão e APIs

Banco de dados distribuídos homogêneos



Replicação em SBDD da Oracle

- Replicação básica
 - São criadas replicações apenas para leitura dos dados. Modificações só podem ser feitas no site primário.
- Replicação avançada (simétrica)
 - Permite atualizações nas replicas das tabelas.
 - Requer um software adicional
 - Advanced Replication option da ORACLE
 - Usa SNAPSHOT

Replicação usando Snapshot

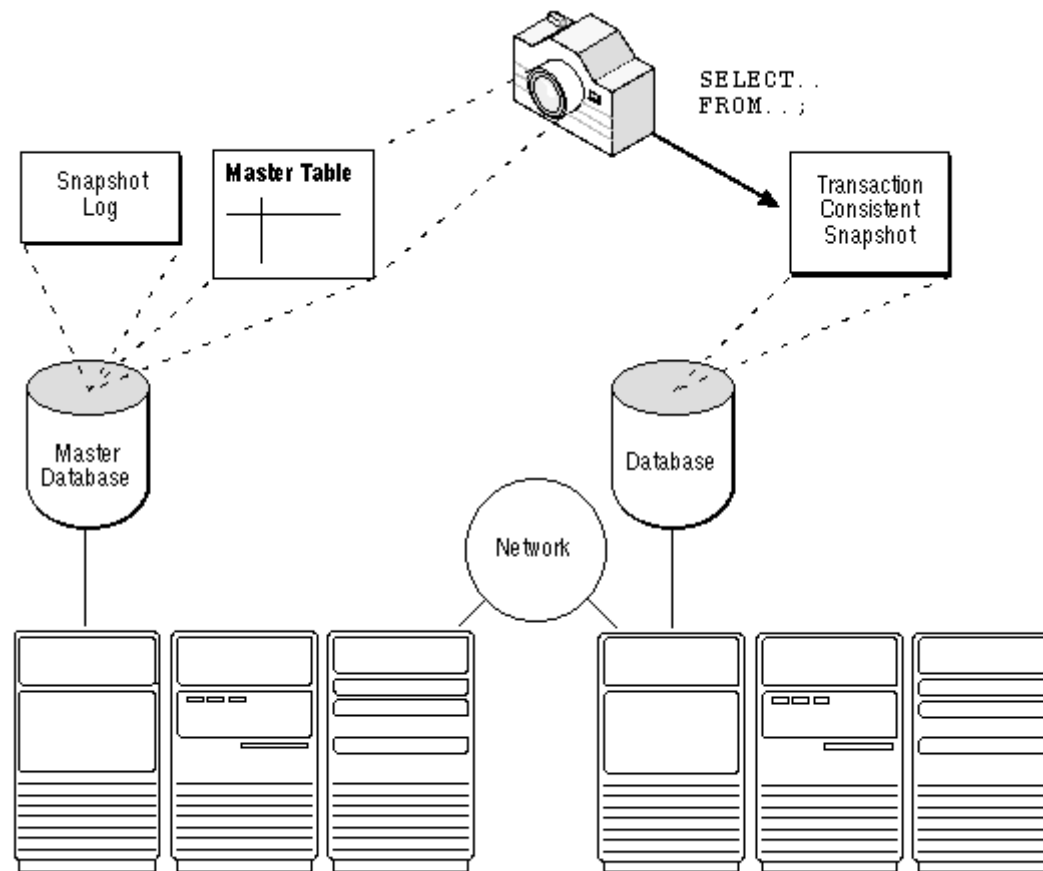
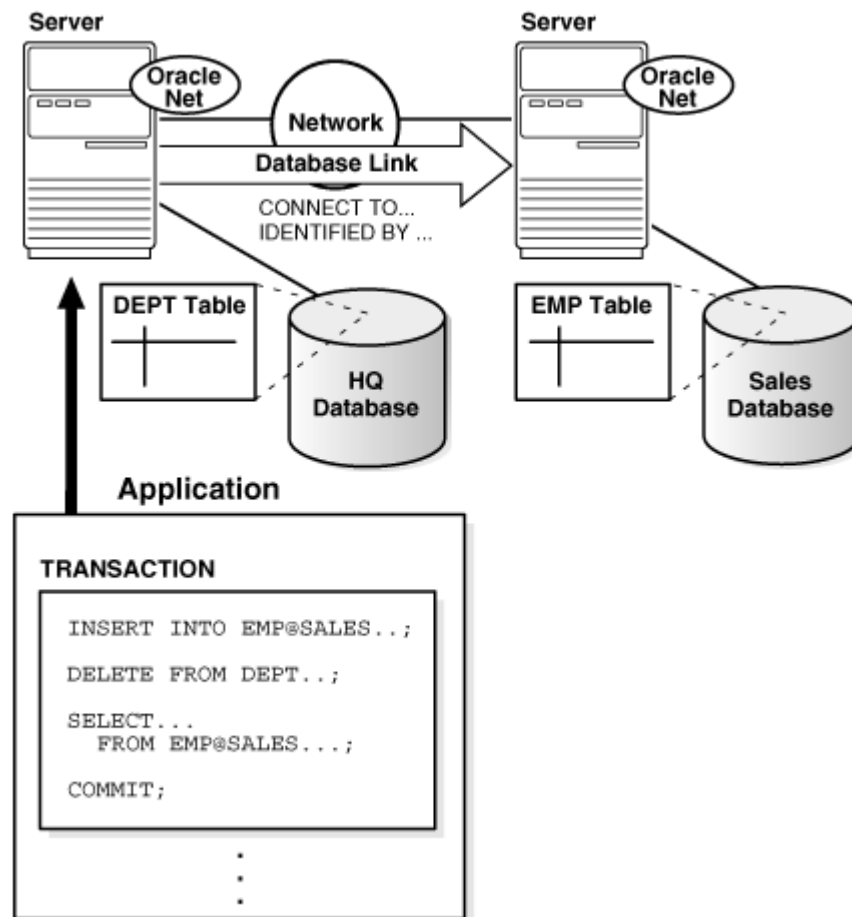


Table Replication Using Snapshots

Banco de dados ORACLE Heterogêneos

- Suporte para SGBDs não ORACLE é feito por meio do
 - Oracle Transparent Gateway
- Database Link
 - É um ponteiro que define a caminho de comunicação unidirecional entre o banco de dados Oracle e outra SGBD.
 - Ex: CREATE PUBLIC DATABASE LINK sales.division3.acme.com USING 'sales1';

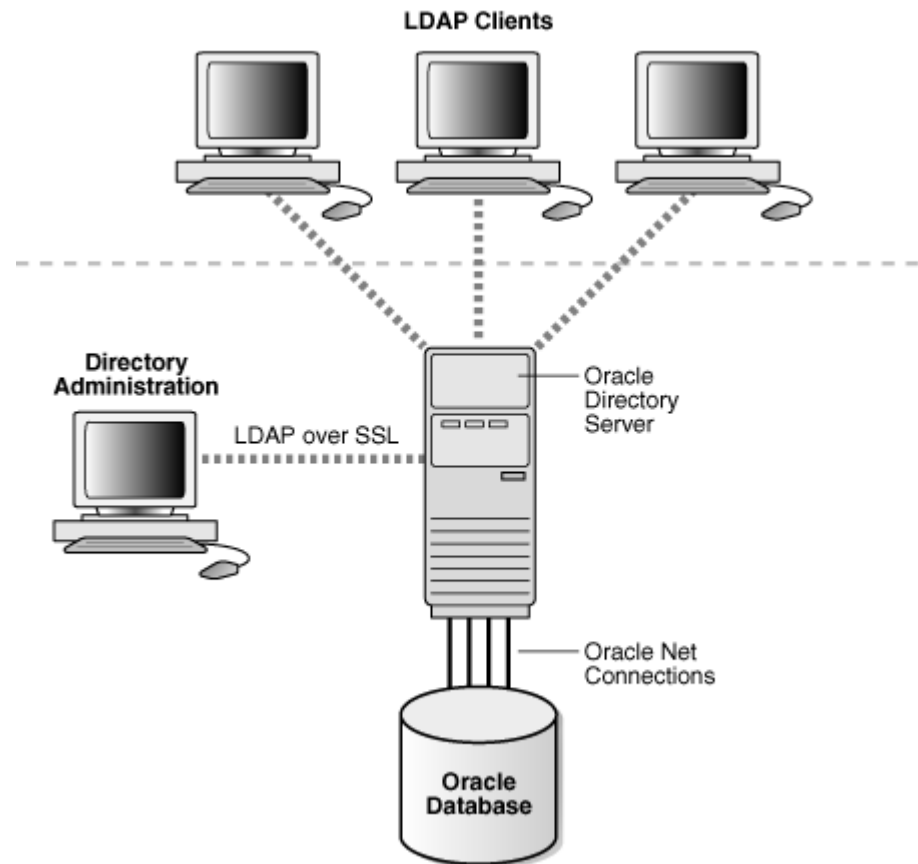
Sistema de BD distribuído da ORACLE



Oracle Open Gateway

- Transações distribuídas
- Acesso transparente à SQL
- SQL pass-through e procedimentos armazenados
- Otimização global de consulta
- Acesso procedimental (PL/SQL)

Oracle Internet Directory



Questão 11 - CESPE - 2014 - TJ-SE - Analista Judiciário - Análise de Sistema

Julgue os seguintes itens, no que se refere ao banco de dados Oracle.

[77] O Oracle utiliza um protocolo de confirmação em duas fases para lidar com transações distribuídas concorrentes.

[78] A replicação em banco de dados Oracle é fornecida em dois níveis: replicação básica e replicação simétrica. Esta última permite que as aplicações atualizem réplicas de tabela por meio de um banco de dados distribuído replicado, e os dados podem ser lidos e atualizados em qualquer sítio.

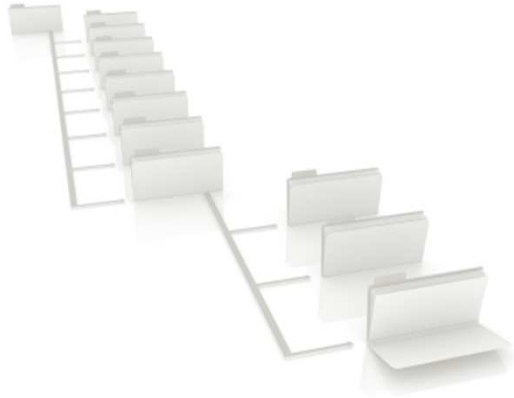
Mensagem final

... e aquilo que pedimos dele
recebemos porque guardamos os
seus mandamentos e fazemos
diante dele o que lhe é agradável.

1 João 3, 22

Muito obrigado!

תודה
Dankie Gracias
Спасибо شكريا
Merci Takk
Köszönjük Terima kasih
Grazie Dziękujemy Děkojame
Ďakujeme Vielen Dank Paldies
Kiitos Tänname teid 谢谢
Thank You Tak
感謝您 Obrigado Teşekkür Ederiz
Σας Ευχαριστούμ 감사합니다
Bedankt ඔබටතෙත
Děkujeme vám
ありがとうございます
Tack



Banco de dados

BDAV02 - Conceitos avançados

Curso Preparatório - ITnerante

Parte 01 – Segurança de banco de dados

Parte 02 – Banco de dados paralelos e distribuídos

Prof. Thiago Cavalcanti





ITnerante 

TIMASTERS 

Simulado 02

BANCO DE DADOS PARALELO E DISTRIBUÍDO

ITnerante 

Questão 01 - CESPE – 2015 - ÓRGÃO: CGE – PI

AUDITOR GOVERNAMENTAL – TEC. DA INFORMAÇÃO

A respeito de banco de dados distribuído, julgue o item a seguir.

[1] Em um ambiente distribuído, os bancos de dados em hosts distintos podem ser acessados durante uma única transação ou consulta. Cada host pode estar fisicamente isolado, sem que esteja logicamente isolado dos demais hosts.

Questão 02 - FCC – 2014 - ÓRGÃO: TJ-AP - ANALISTA JUDICIÁRIO - BANCO DE DADOS - DBA

Na replicação de tabelas em um banco de dados relacional,

- a) cada tabela replicada não pode ser acessada (para leitura ou escrita), por mais do que um usuário, simultaneamente.
- b) quando uma tabela tem seus dados modificados, todas as réplicas dessa tabela devem também refletir tal modificação.
- c) quando uma réplica é acessada para leitura, as demais réplicas são bloqueadas para leitura.
- d) o número máximo teórico de réplicas possíveis que uma tabela pode ter é 5.
- e) as diversas réplicas devem ser salvas em locais com sistemas gerenciadores de bancos de dados distintos entre si.

Questão 03 - FCC – 2014 - ÓRGÃO: TJ-AP - ANALISTA JUDICIÁRIO - BANCO DE DADOS - DBA

No particionamento ou fragmentação vertical de uma tabela de um banco de dados relacional

- a) separam-se, obrigatoriamente, atributos do tipo numérico de atributos do tipo literal.
- b) cada partição ou fragmento inclui alguns dos registros da tabela original.
- c) acrescenta-se um atributo que irá conter um código denominado de check-sum dos demais atributos.
- d) cada atributo é codificado e armazenado, visando, dessa forma, a proteção dos dados.
- e) cada partição ou fragmento inclui alguns dos atributos da tabela original.

Questão 04 - FCC - 2008 - Órgão: METRÔ-SP- Prova: Analista Treinee - Ciências da Computação

Em termos de banco de dados, é correto afirmar:

- a) No controle de segurança do tipo discricionário, a cada objeto de dados é assinalado certo nível de classificação, e cada usuário recebe certo nível de liberação.
- b) A independência do hardware não é um dos objetivos da implementação de um sistema de bancos de dados distribuídos, mas sim a obtenção da independência da fragmentação.
- c) Uma das regras de integridade do modelo relacional afirma que nenhum campo que participe da chave primária de uma tabela básica pode aceitar valores nulos.
- d) Uma das vantagens dos sistemas de banco de dados distribuído é sua capacidade de tornar perceptível aos usuários os níveis de sua arquitetura performática em relação aos sistemas não distribuídos.
- e) A linguagem de definição de dados oferece suporte à declaração de objetos do banco de dados, enquanto a linguagem de estruturação de dados admite o processamento desses objetos.

Questão 05 - CESPE - 2008 - Órgão: STF - Prova: Analista Judiciário - Tecnologia da Informação

O armazenamento e a recuperação de grandes quantidades de dados é um trabalho importante e muito explorado em um sistema gerenciador de banco de dados (SGBD). Com relação aos conceitos que envolvem esse sistema, julgue os itens que se seguem.

[1] Em um sistema de banco de dados distribuídos, a comunicação entre nós pertencentes ao sistema é feita de maneira não transparente para o usuário do banco.

Questão 06 - FCC - 2009 - Órgão: PGE-RJ Prova: Técnico Superior de Análise de Sistemas e Métodos

São dois princípios fundamentais e ideais dos bancos de dados distribuídos, a

- a) independência do sistema operacional e a independência do SGBD.
- b) independência de replicação e o processamento de consultas centralizado.
- c) autonomia distribuída e a dependência do SGBD.
- d) dependência de replicação e a não-dependência de um site central.
- e) autonomia local e o gerenciamento de transações centralizado.

Questão 07 - FCC - 2013 - Órgão: MPE-MA Prova: Analista Ministerial - Banco de Dados

Um tipo de banco de dados é representado pelos bancos de dados relacionais distribuídos, nos quais pode ser feita a fragmentação de dados, que consiste em

- a) criptografar todas as tabelas do banco de dados utilizando uma chave pública.
- b) dividir as tabelas do banco de dados e armazenar cada parte em um local (site) diferente.
- c) excluir os registros das tabelas que possuam atributos com valores nulos.
- d) excluir todas as tabelas que não possuam chave estrangeira.
- e) replicar todas as tabelas do banco de dados em todos os locais (sites).

Questão 08 - CESPE - 2009 - Órgão: TCE-TO Prova: Analista de Controle Externo - Proc. de Dados

Com relação a bancos de dados distribuídos, assinale a opção incorreta.

- a) A replicação total de uma relação ocorre quando esta é armazenada em todos os sites.
- b) Na fragmentação horizontal, cada esquema é alocado em um ou mais fragmentos.
- c) A fragmentação horizontal e a vertical podem ser combinadas.
- d) Uma vantagem da replicação é a reduzida taxa de transferência.
- e) Na fragmentação vertical, o esquema de uma relação é dividido em esquemas menores.

Questão 09 - CESPE - 2009 - Órgão: INMETRO Prova: Analista Metrologia e Qualidade – Des. de Sistemas

Quanto aos tópicos avançados em tecnologia da informação, julgue os itens a seguir.

[1] Em uma organização composta por várias unidades de negócio geograficamente distribuídas e que utiliza um sistema de bancos de dados distribuídos, o uso de fragmentação horizontal é recomendado quando há grande heterogeneidade de atividades realizadas em uma base de clientes comum a todas as unidades, enquanto a fragmentação vertical é indicada quando as várias unidades realizam basicamente as mesmas atividades em uma base de clientes particionados entre as unidades.

Questão 10 - FEPESE – 2010 - Órgão: UDESC - Prova: Analista de Sistemas

A respeito de bancos de dados distribuídos, é correto afirmar:

- a) a replicação de dados em diversos nodos integrantes da arquitetura distribuída é sempre uma boa prática de projeto de bancos de dados distribuídos, pois torna qualquer dado sempre disponível em qualquer nodo.
- b) a falha de um nodo integrante da arquitetura distribuída sempre causa o colapso de todas as transações distribuídas em execução.
- c) consultas distribuídas são sempre processadas em um único nodo integrante da arquitetura distribuída.
- d) uma das vantagens da fragmentação de dados de uma relação em diversos nodos integrantes de uma arquitetura distribuída é manter o dado disponível no nodo onde ele é mais frequentemente acessado.
- e) o controle da execução concorrente de transações distribuídas é sempre responsabilidade de um único nodo integrante da arquitetura distribuída.



ITnerante 

TIMASTERS 

Questões - Gabarito

Questões do curso BDAV02



Questões – SBDDs e SBDPs

Questões

1. C
2. E
3. C
4. E
5. C
6. E
7. C
8. E
9. E
10. C
11. C C

Simulado

1. C
2. B
3. E
4. C
5. E
6. A
7. B
8. B
9. E
10. D



ITnerante 

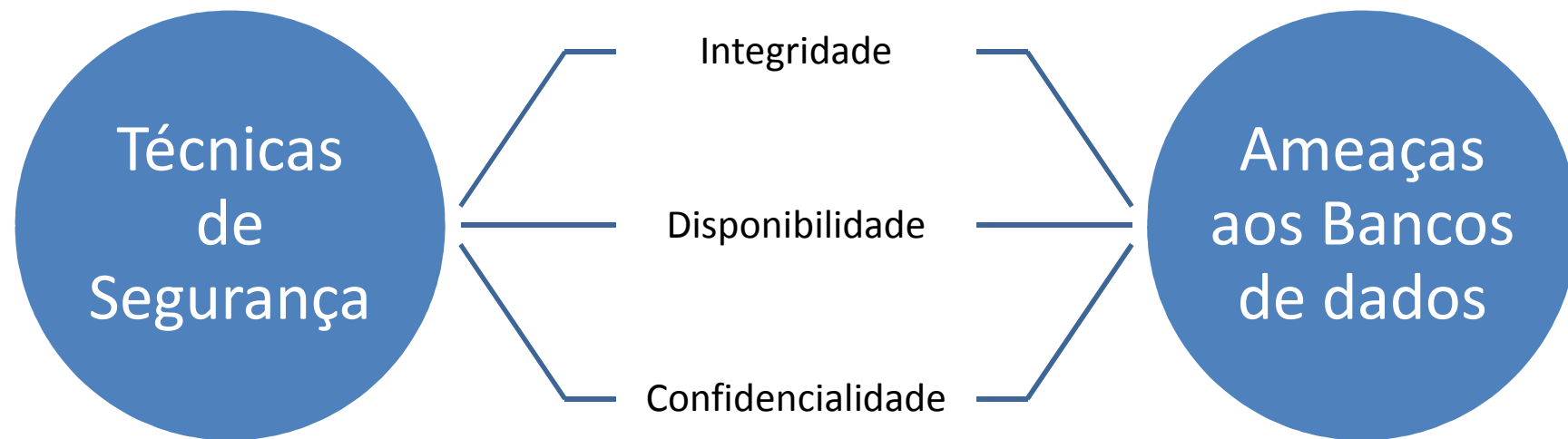
TIMASTERS 

Memorex

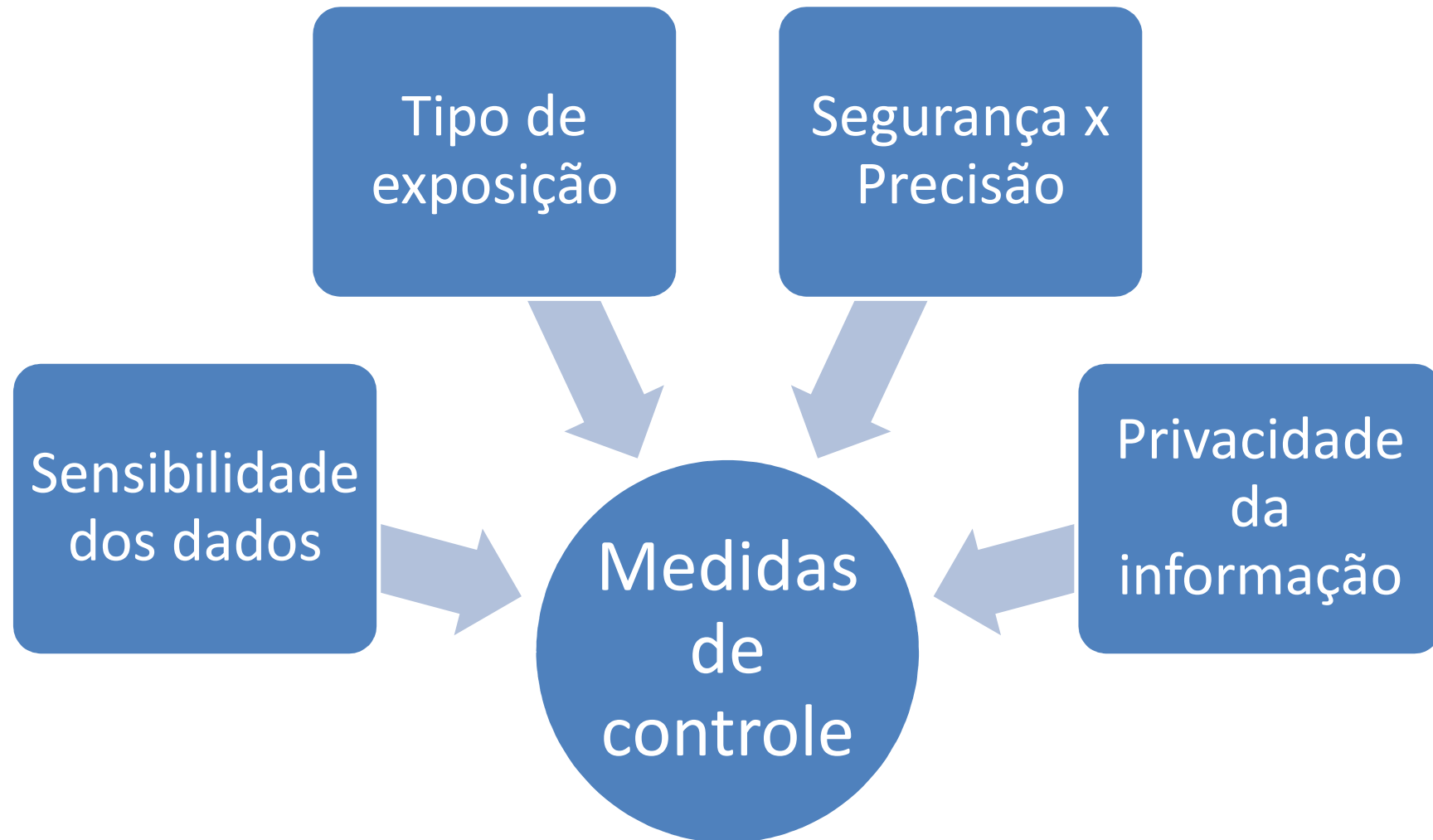
Revisão completa do curso



Segurança em Banco de Dados



Conceitos



Controles

Acesso ao SGBD ou BD (Autenticação)

Conta e Senha

Autorização a objetos

Partes específicas

Discricionário (DAC)

Concessão/Revogação de privilégios

SQL: Grant e Revoke

Obrigatório (MAC)

Segurança Multinível

Pode usar: filtragem ou poli-
instanciação

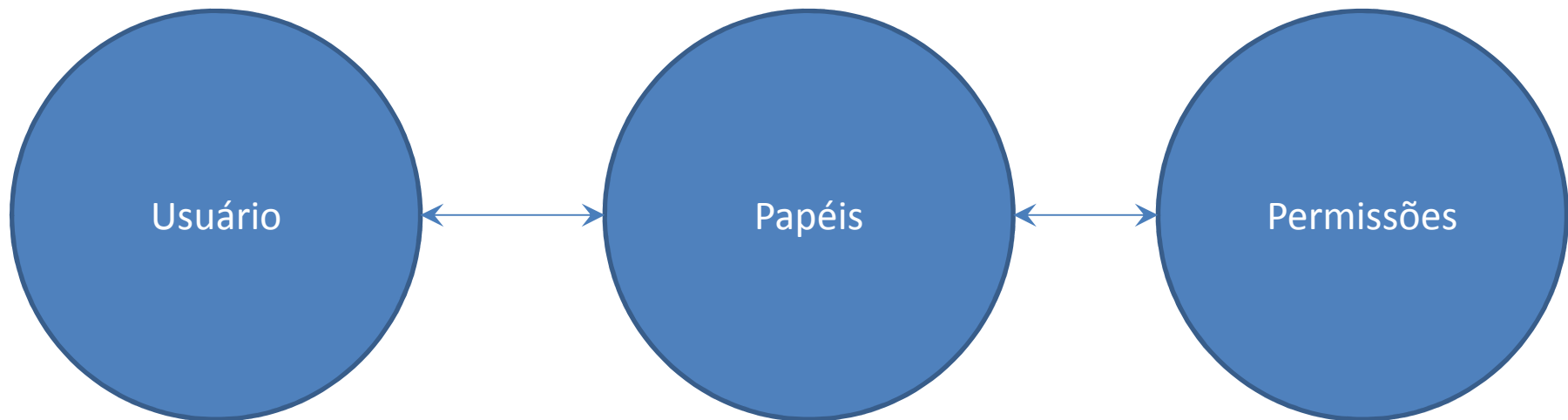
Classifica usuários e dados em
classes

Regras para fluxo de
informação entre níveis



Controle de acesso baseado em papéis (RBAC)

- Hierarquia entre papéis
- Exclusão mútua de papéis
- Segurança baseada em linha e rótulos



Injeção SQL

- O objetivo é injetar linguagem SQL maliciosa dentro do que a aplicação usa para fazer query no banco de dados.
- Métodos de injeção
 - Manipulação de SQL
 - Injeção de código
 - Injeção de chamada de função

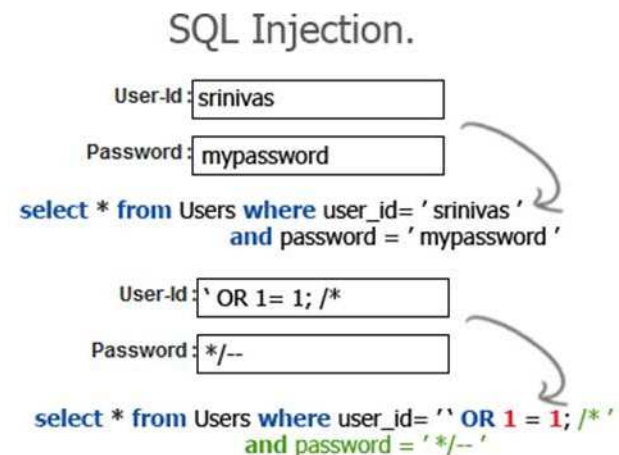
SQL Injection.

User-Id:
Password:

`select * from Users where user_id= 'srinivas' and password = 'mypassword'`

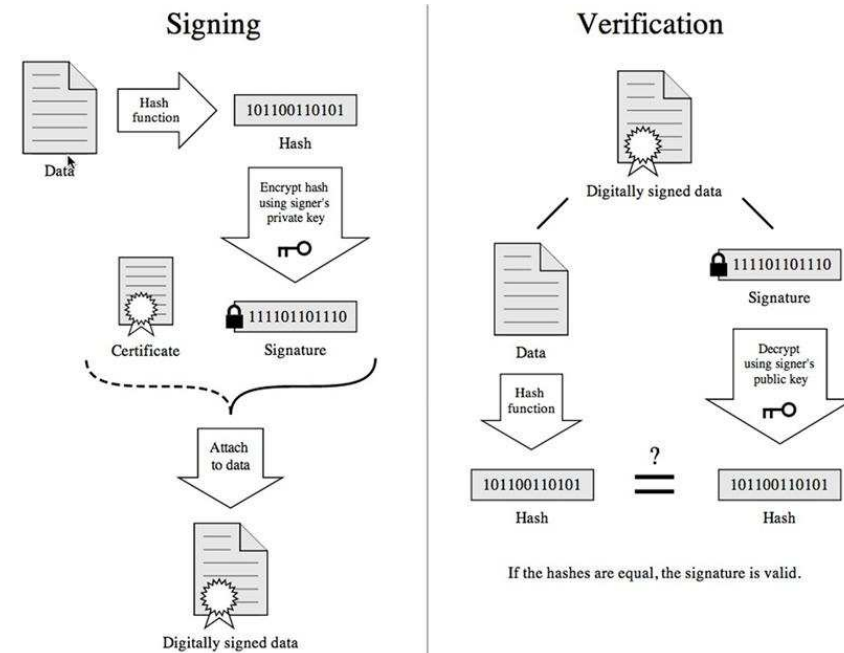
User-Id:
Password:

`select * from Users where user_id= '' OR 1 = 1; /*' and password = '*/--'`



Conceitos relacionados ao controle de fluxo

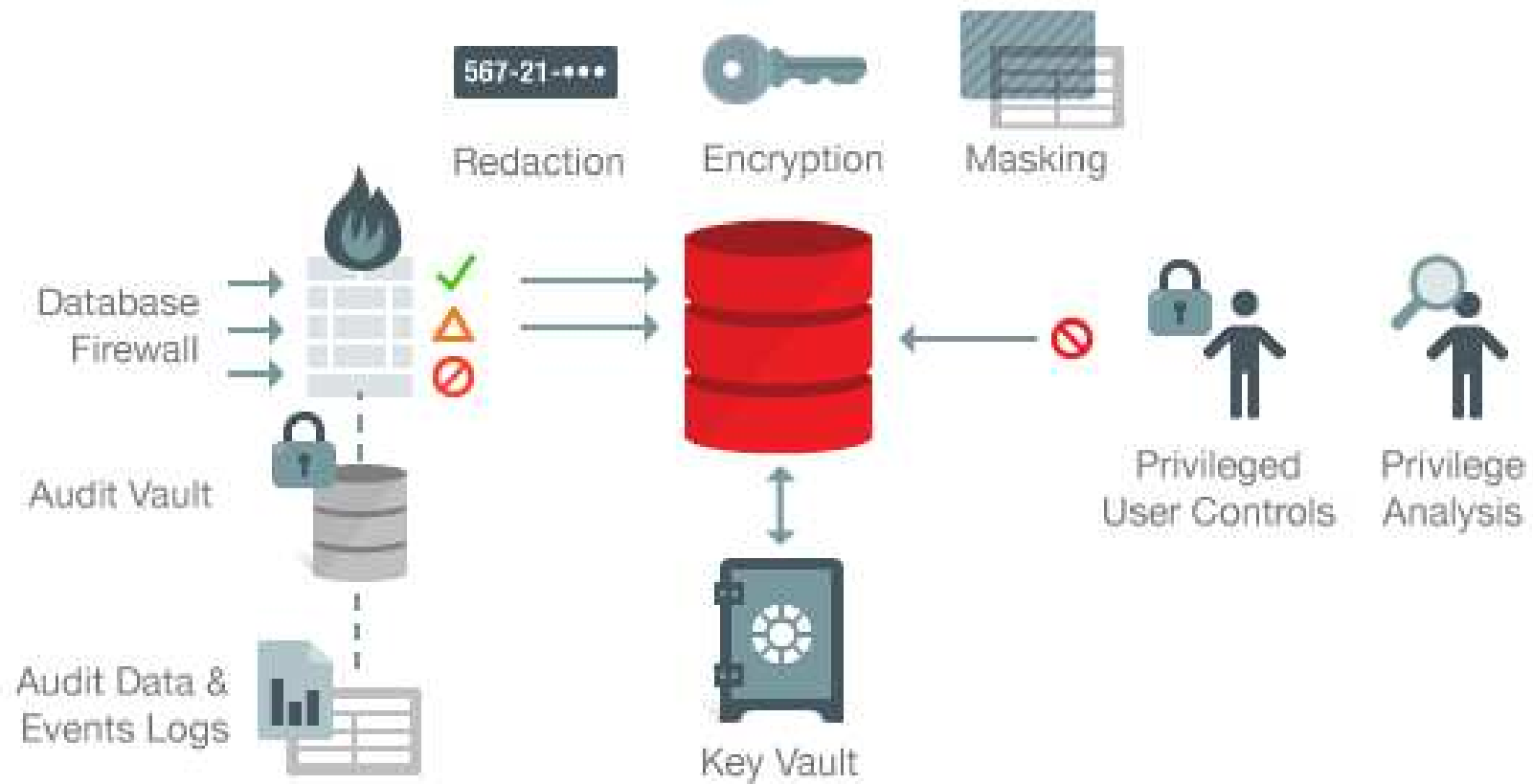
- Canais secretos
- Criptografia
 - Simétrica ou assimétrica
- Assinatura Digital
- Certificado Digital



Segurança no Oracle 11g

- Contas de usuários
- Métodos de autenticação
- Privilégios e papéis (roles)
- Aplicação das políticas de segurança
- Virtual Private Database (VPD)
- Criptografia
- Auditoria nas atividades do banco de dados

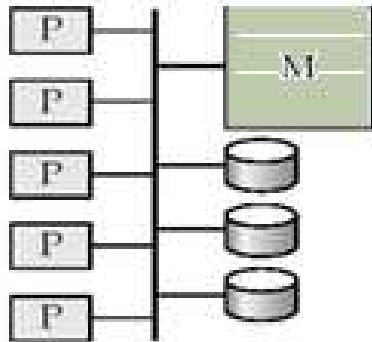
Key Oracle 12c Security



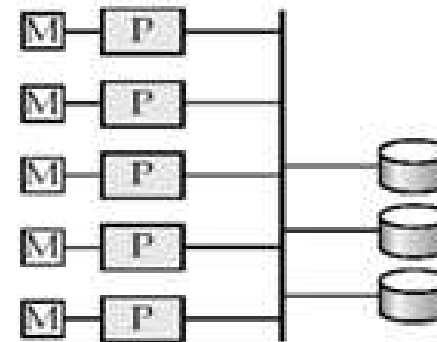
Sistemas paralelos

- Melhoram as velocidades:
 - De processamento
 - De Entrada e Saída (E/S)
 - Usando várias CPUs e discos em paralelo.
- Muitas operações são realizadas em paralelo
- Medidas de desempenho
 - Throughput – número de tarefas em determinado intervalo de tempo
 - Tempo de resposta – tempo para completar uma tarefa determinada

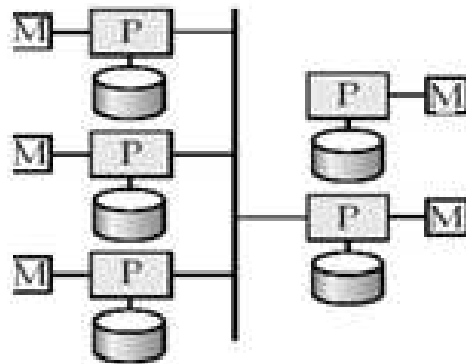
Banco de dados paralelos



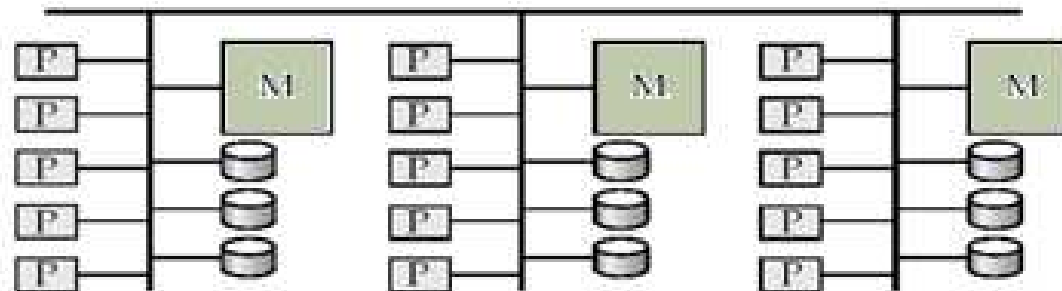
(a) shared memory



(b) shared disk



(c) shared nothing



(d) hierarchical

Banco de dados distribuído

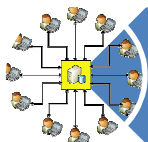
- Uma coleção de múltiplos bancos de dados logicamente inter-relacionados, distribuídos por um rede de computadores, e um sistemas de banco de dados distribuídos (SGBDD)
 - **SGBDD** – um sistema que gerencia o BDD enquanto torna a distribuição transparente pra o usuário.



Regras associadas ou objetivos secundários



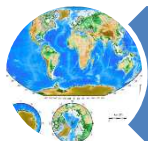
Autonomia local



Não dependência de um site central



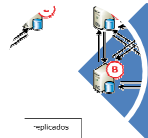
Operação contínua



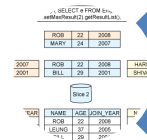
Independência de localização



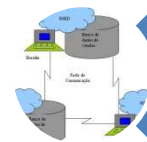
Independência de fragmentação



Independência de replicação



Processamento de consultas distribuído



Gerenciamento de transações distribuídas



Independência de Hardware



Independência de sistema operacional

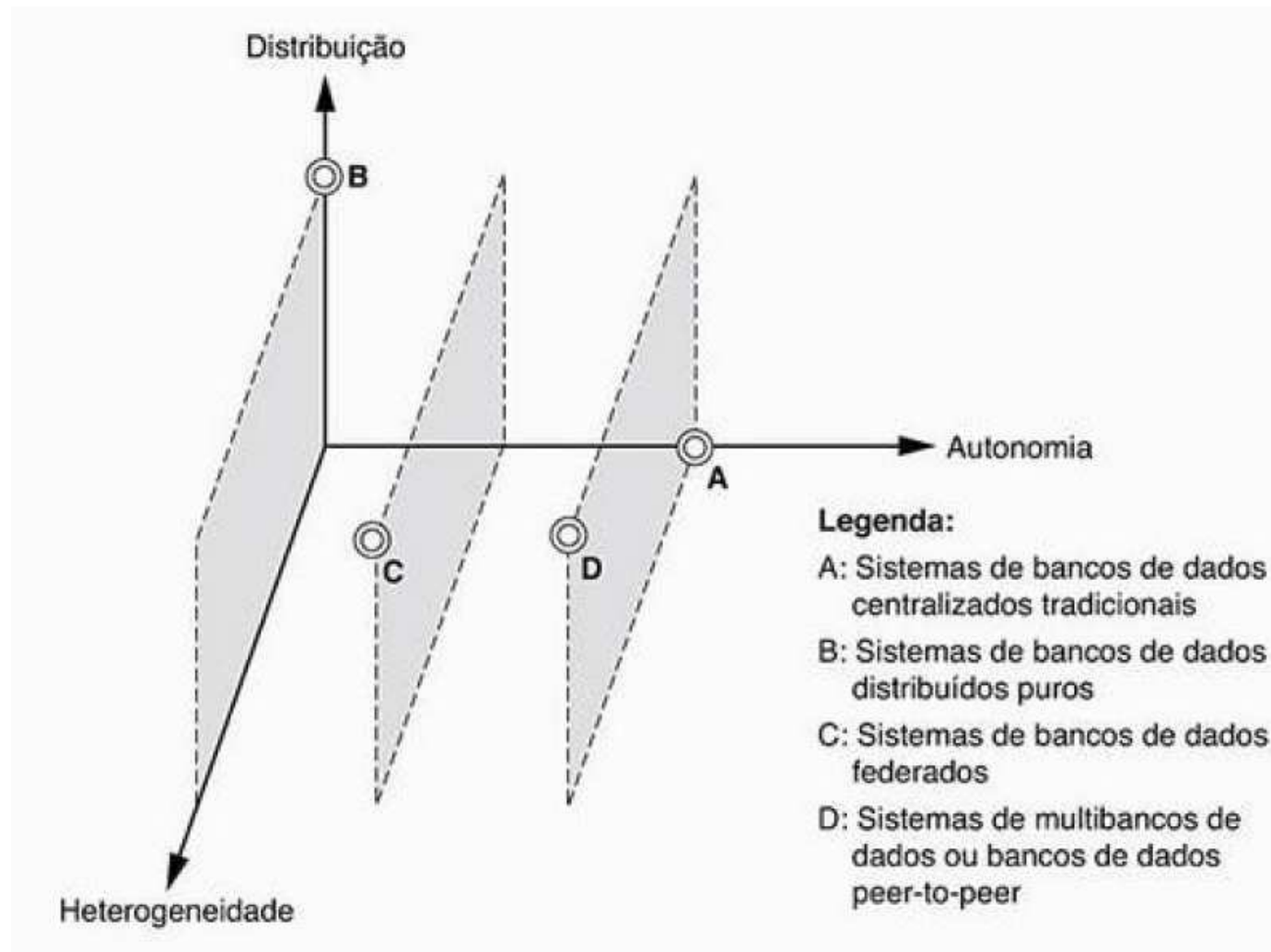


Independência de rede



Independência de SGBD

Classificação dos SBDD



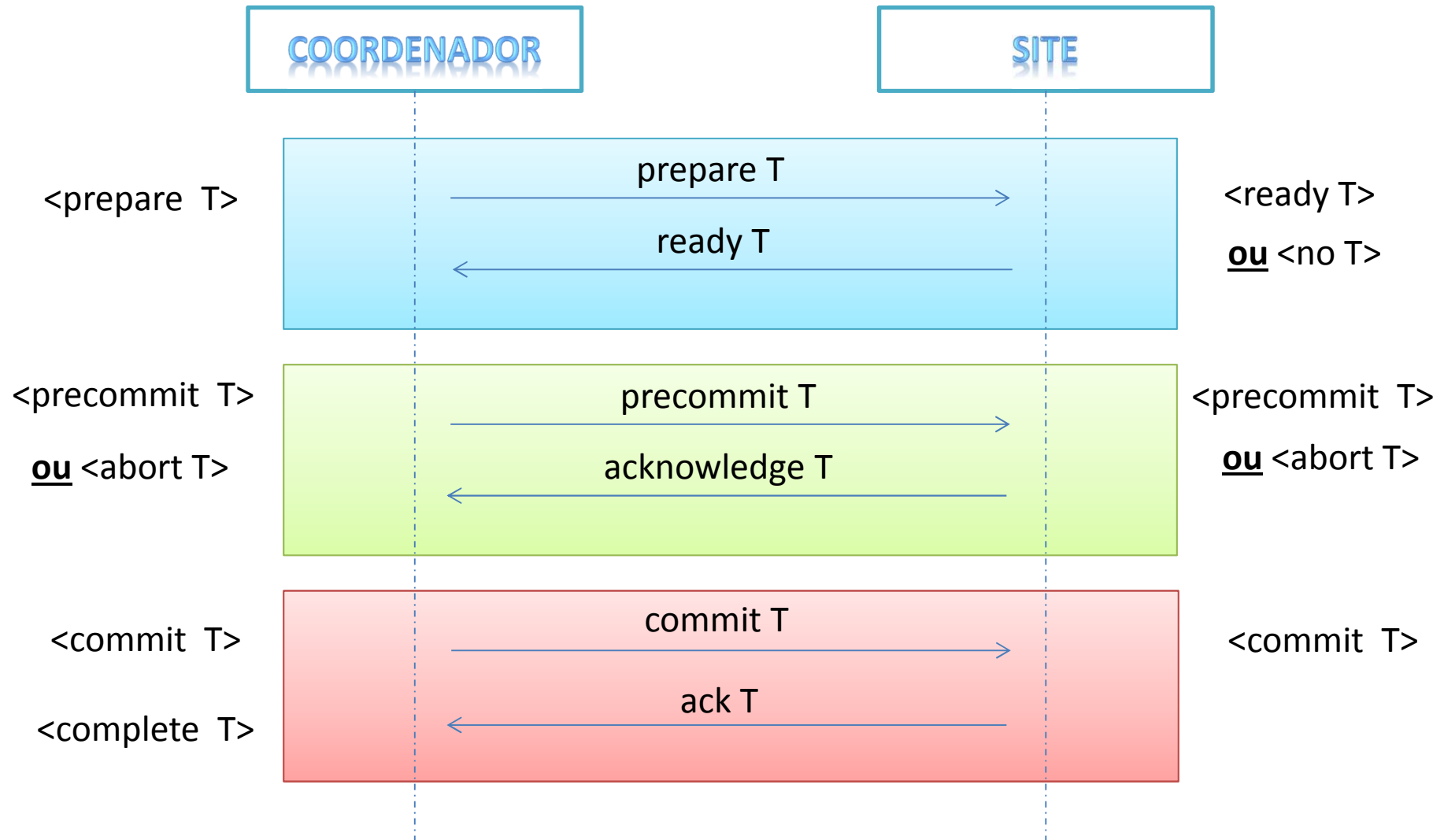
Fragmentação de dados

- A informação sobre a fragmentação, replicação e alocação de dados é armazenada no diretório global.
- Fragmentação horizontal
 - Subconjunto de tuplas de uma relação
 - Ex. Um site para cada departamento
- Fragmentação vertical
 - Divide a relação verticalmente por colunas
 - Cada fragmento mantém apenas certos atributos
 - Ex: Informações pessoais e de trabalho de um FUNC

Replicação e alocação de dados

- BDD Totalmente replicado
 - Melhora a disponibilidade e **desempenho de recuperação**
 - **Desvantagem:** Operações de atualização!
- **Alocação não redundante**
- Replicação parcial
 - Comum em profissionais de vendas
- Esquema de replicação
 - Descreve a replicação dos fragmentos.
 - Distribuição de dados

Commit em três fases





ITnerante 

TIMASTERS 

Memorex

Revisão completa do curso

