Comparaison de la sécurité entre les SGBD DB2 et Oracle

Présenté par : Guy Jobin
Michel Guy Paiement

Date: 19 avril 2004
Cours: INF7115

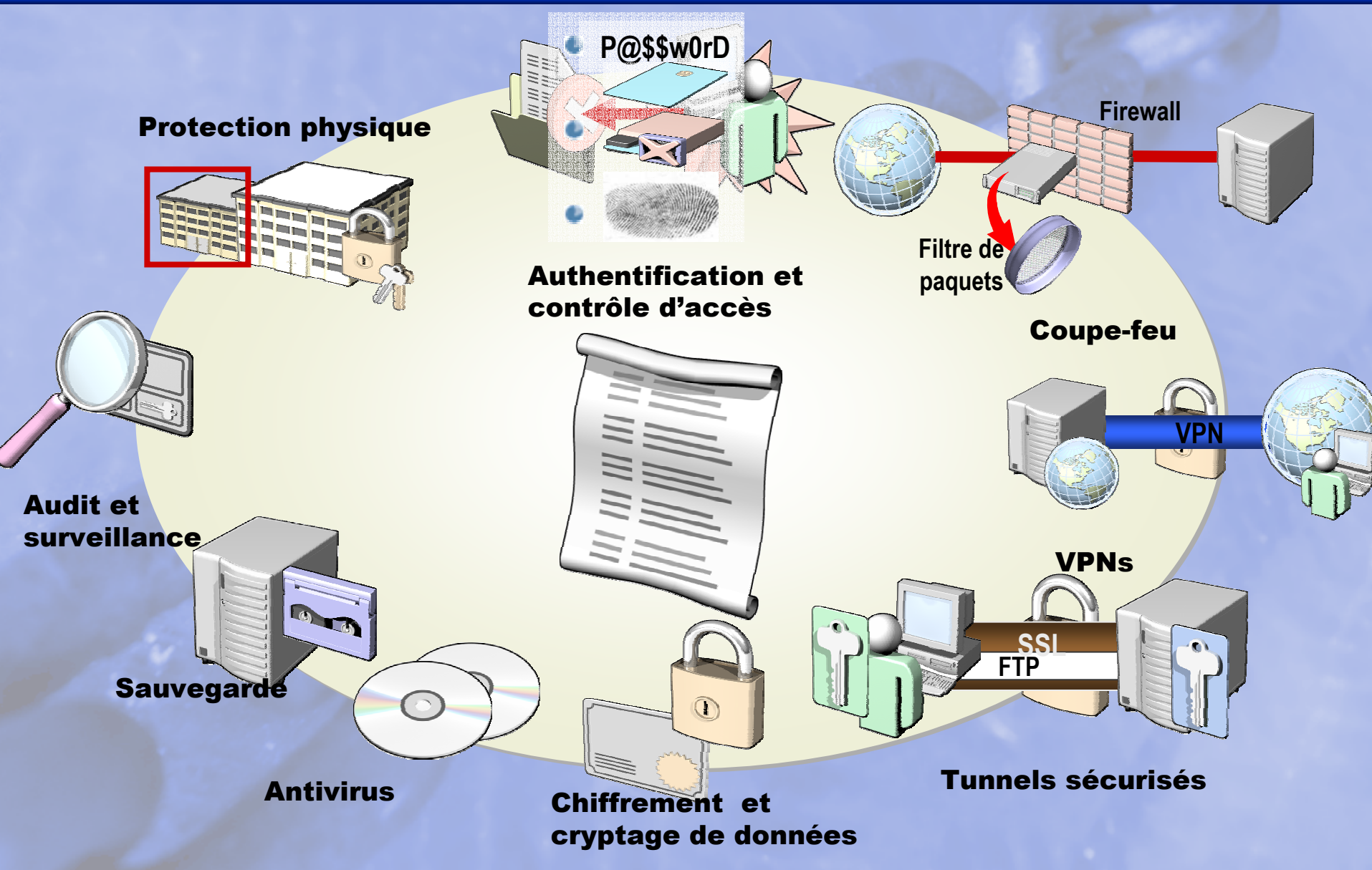
Plan de présentation

- **Introduction**
- **Présentation des concepts de bases de la sécurité**
- **Applications des critères de sécurité aux SGBD étudiés**
- **Conclusion (Présentation de la grille de comparaison)**

Introduction

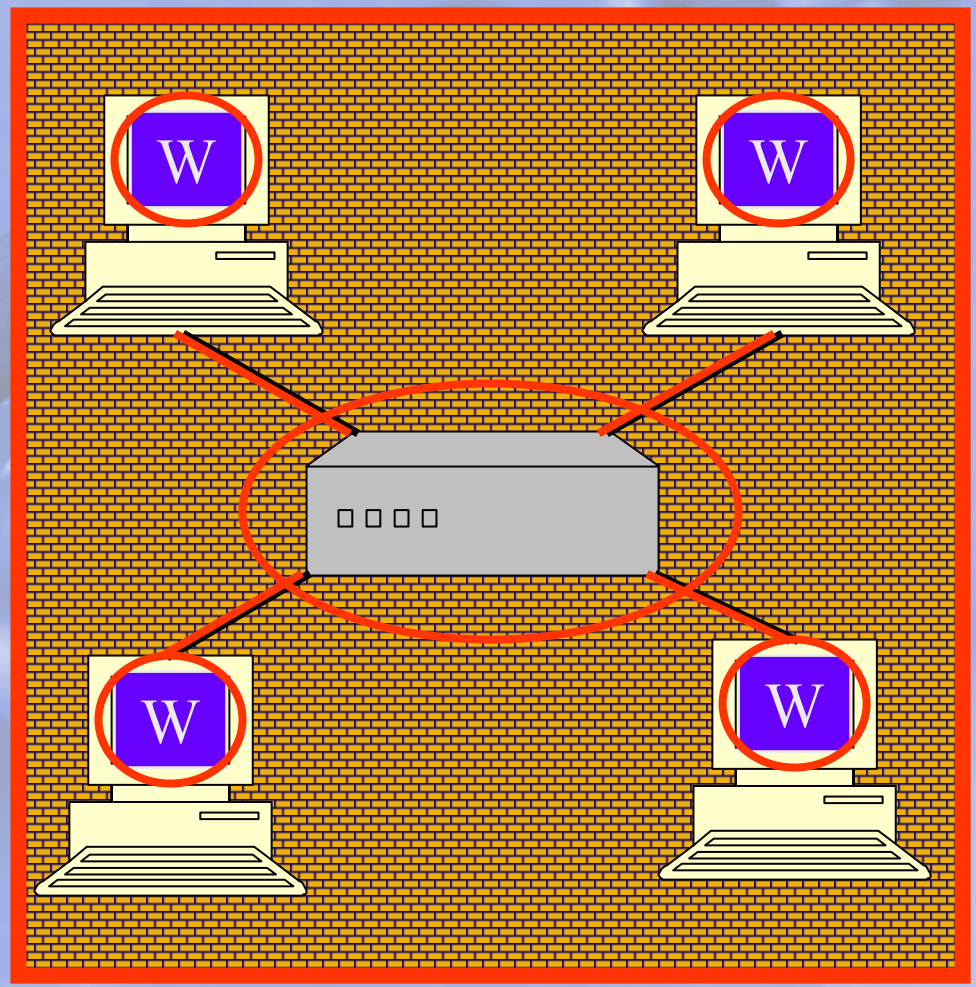
- **La sécurité?**
  - La Grande Muraille de Chine
  - Incidents de sécurité

Sécurité et technologie

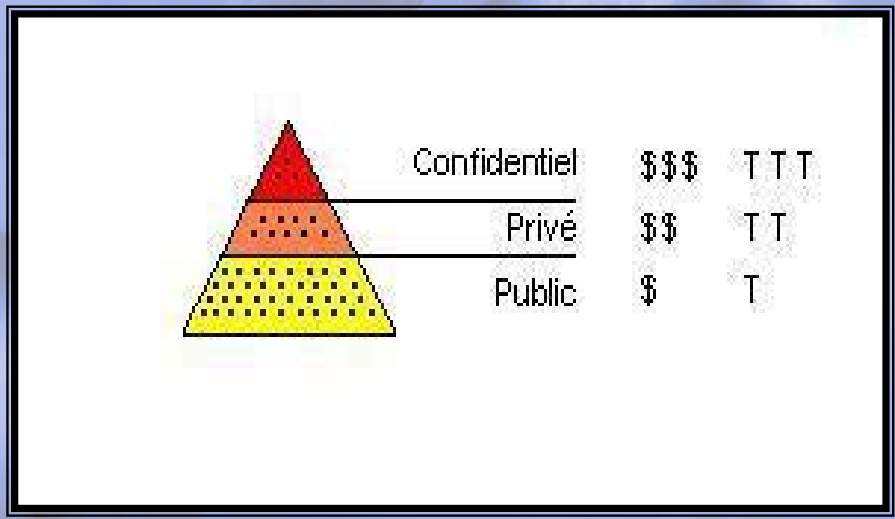


Domaines de définition de la sécurité informatique

- La sécurité physique
- La sécurité de l'exploitation
- La sécurité logique
- La sécurité applicative
- La sécurité des télécommunications



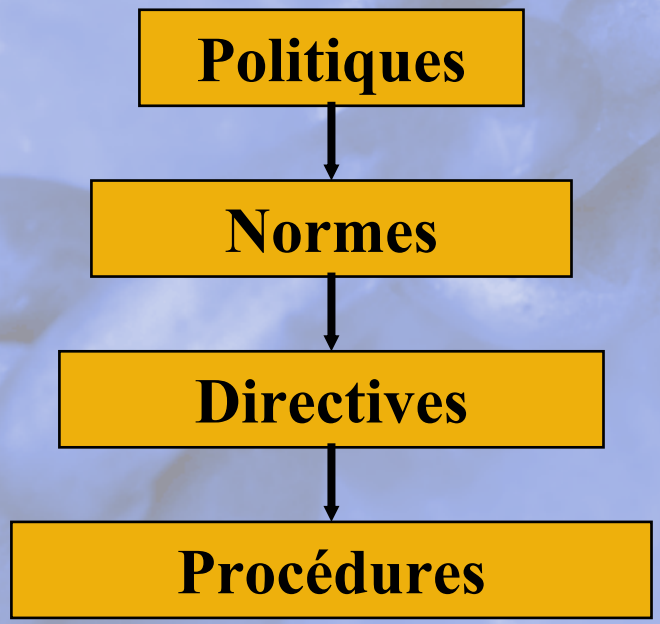
Classification des ressources

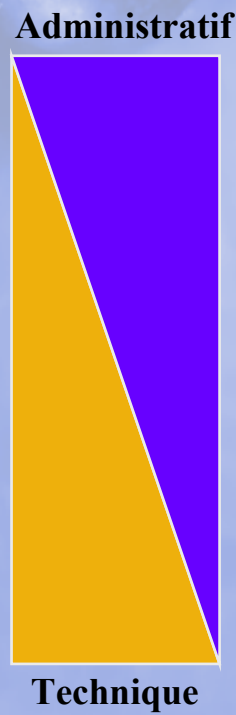


Les processus administratifs

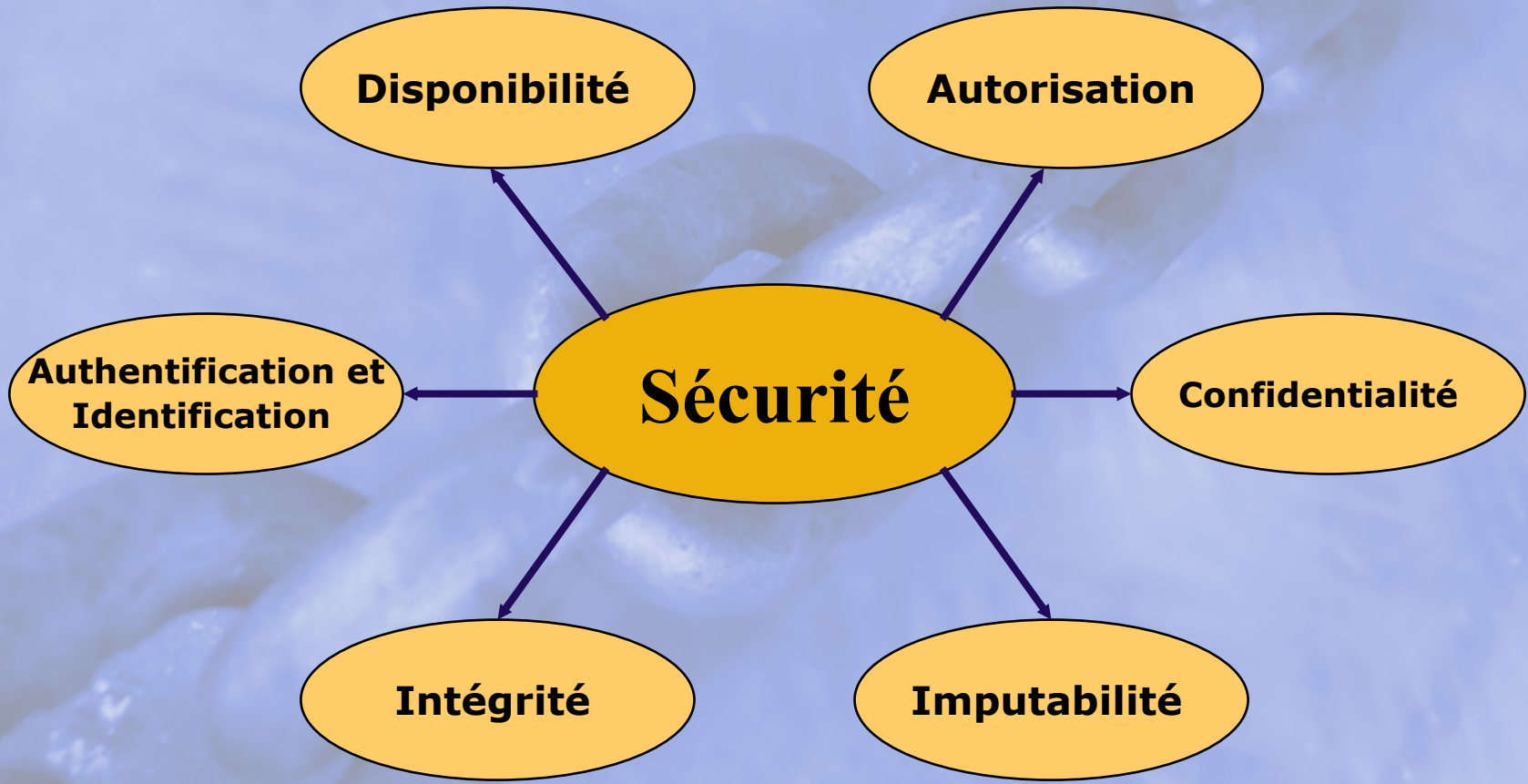
- **Contrôles :**

  administratifs (politiques et procédures, conscientisation, vérification, supervision)



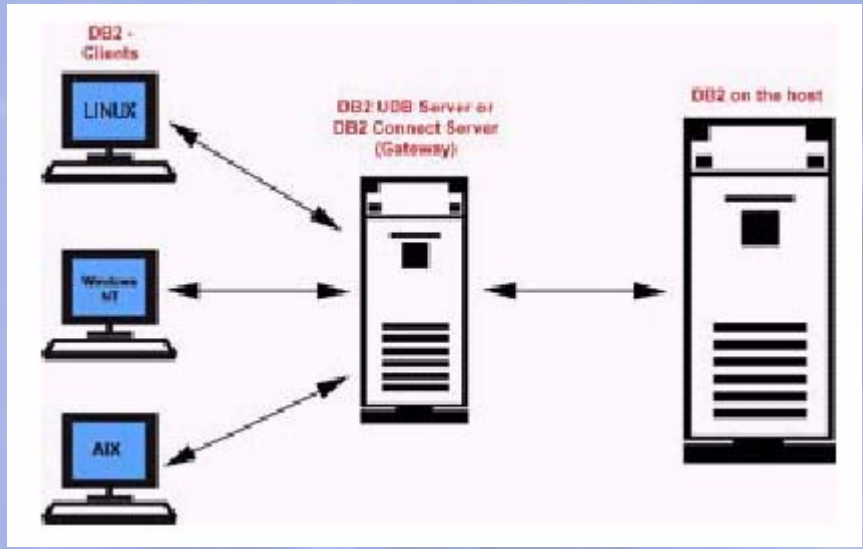


Les critères de sécurité



Authentification : Code d'Accès + Authentifiant

DB2 [1]



Type
SERVER
SERVER_ENCRYPT
CLIENT
*KERBEROS
*KRB_SERVER_ENCRYPT

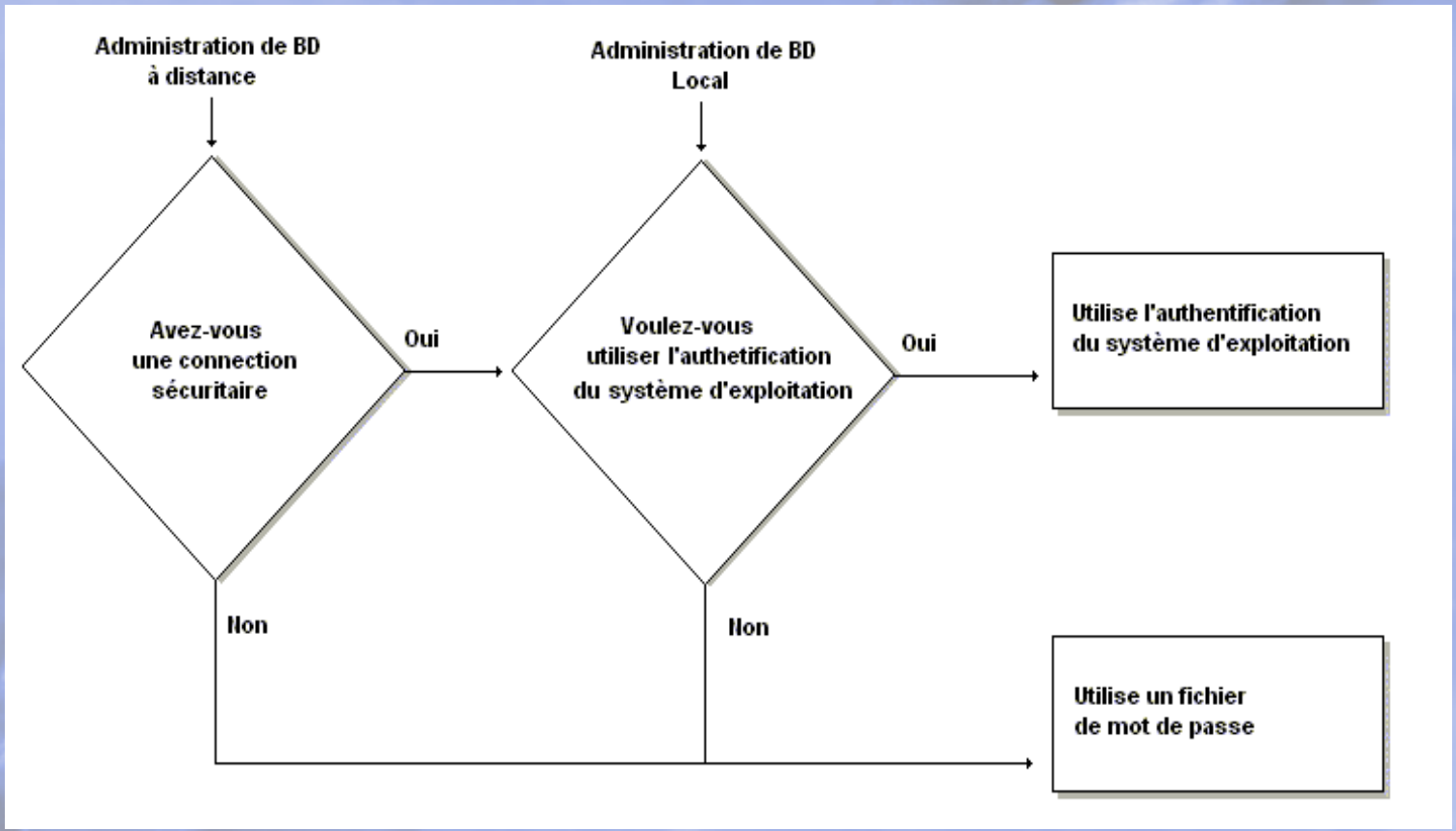
Authentification : Code d'Accès + Authentifiant

DB2 [2]

Usager : LID + Groupes (rôles)

Authentification

Oracle 1



Authentification

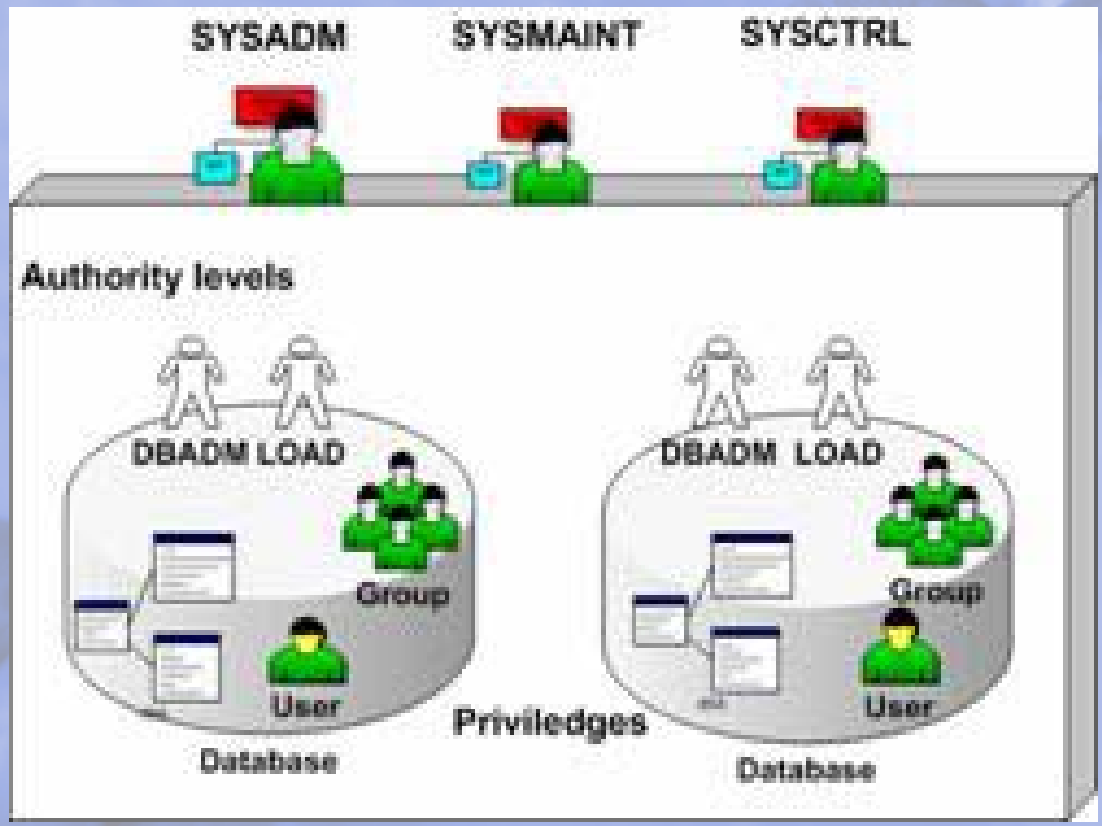
Oracle 2

Le services d'authentification de sqlnet.ora inclus :

- **BEQ**
- **KERBEROS5**
- **CYBERSAFE**
- **RADIUS**
- **IDENTIX**
- **SECURID**

Autorisation

DB2 1



Autorisation (privilèges)

DB2 2

Privilege name	Relevant object(s)
CONTROL	Table, View, Index, Package, Alias, Distinct Type, User Defined function, Sequence
DELETE	Table, View
INSERT	Table, View
SELECT	Table, View
UPDATE	Table, View
ALTER	Table
INDEX	Table
REFERENCES	Table

BIND	Package
EXECUTE	Package, Procedure, Function, Method
ALTERIN	Schema
CREATEIN	Schema
DROPIN	Schema

Autorisation

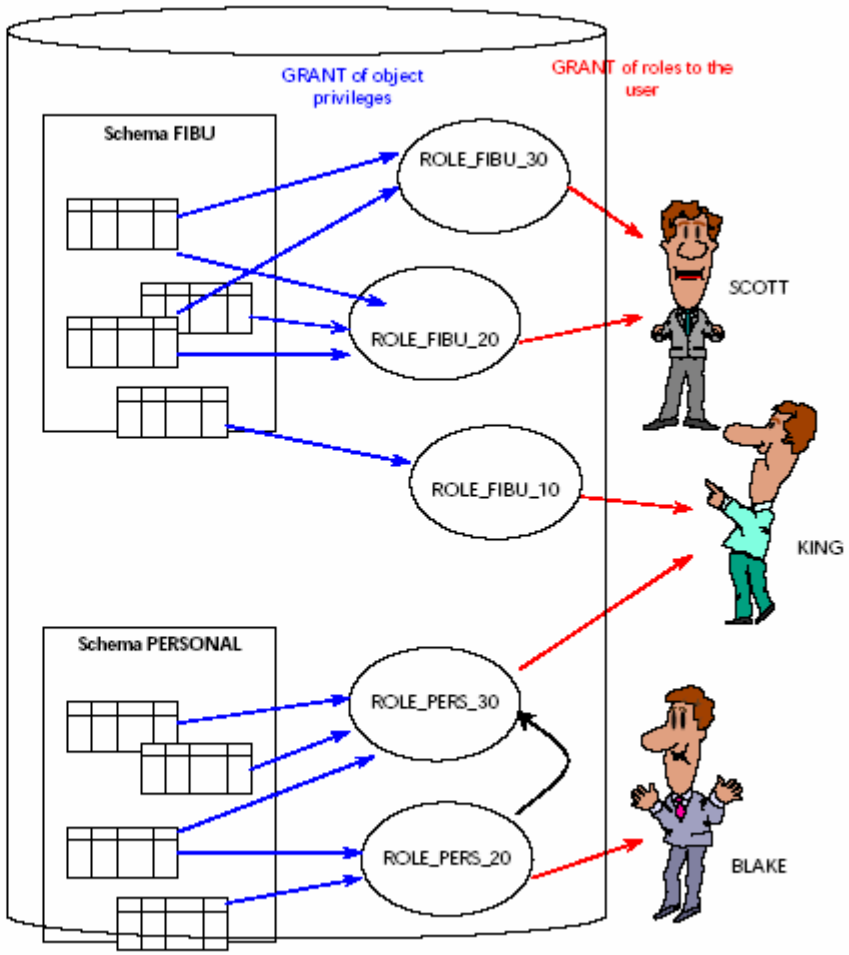
Oracle 1

Privilège	Action
Select	Voir l'information à l'intérieur d'une table ou d'une vue
Insert	Insérer de nouvelles lignes d'informations à l'intérieur d'une table ou d'une vue
Update	Modifier une ou plusieurs colonnes d'informations à l'intérieur d'une table ou d'une vue
Delete	Effacer une ou plusieurs lignes d'informations à l'intérieur d'une table ou d'une vue
Alter	Changer la définition d'un objet
Execute	Compiler, exécuter ou accéder à des procédures ou des fonctions référencées à l'intérieur d'un programme
Read	Lire des fichiers dans un répertoire
Reference	Créer une contrainte qui fait référence à une table
Index	Créer un index sur une table

Autorisation

Oracle 2

- Privilèges:
  - Sur des objects:
    grant select , update , etc …
  - System:
    connect, create table
- Les privilèges peuvent être donnés directement à un utilisateur ou via un rôle
- On associe à un rôle un ensemble de privilèges system ou objet



Autorisation

Oracle 3

Compte utilisateurs venant avec la DB

Compte	DBA	RESOURCE (unlimited tablespace)	execute any procedure	select any table	select any dictionary	exempt access policy	alter system
CTXSYS	✓	✓	✓	✓	✓		✓
DBSNMP					✓		
LBACSYS		✓	✓	✓			
OLAPDBA		✓		✓	✓		
OLAPSVR		✓		✓	✓		
OLAPSYS		✓		✓	✓		
ORDPLUGINS		✓					
ORDSYS		✓					
OUTLN		✓	✓				
MDSYS	✓	✓	✓	✓	✓		✓
WKSYS	✓	✓	✓	✓	✓		✓
XDB				✓		✓	

Confidentialité

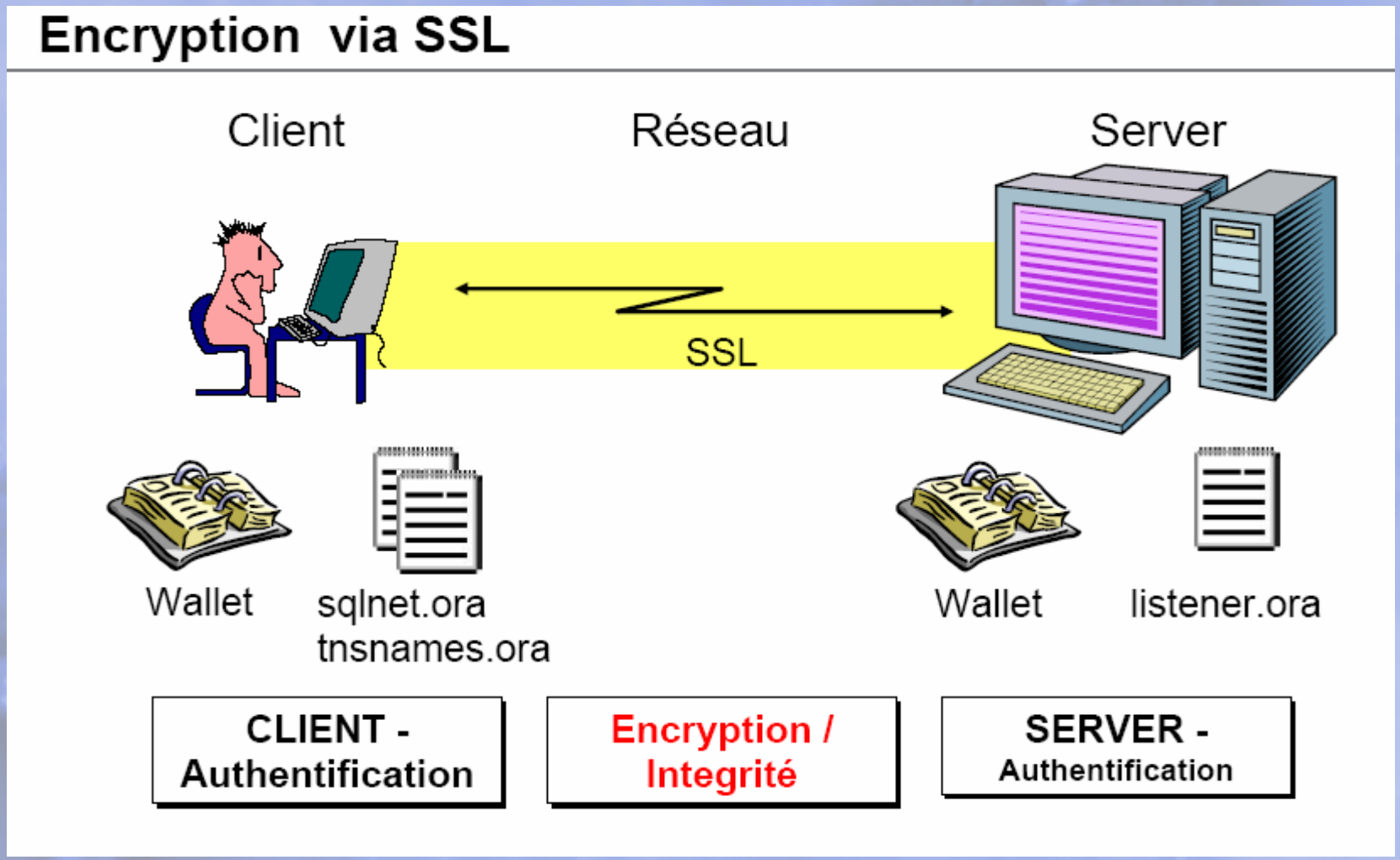
DB2

DB2 laisse au système d'exploitation cette responsabilité.

DB2 permet néant moins de protéger les données lors d'export

Confidentialité

Oracle 1



Confidentialité

Oracle 2

Configuration du crypto_checksum_*

- Server et Client Parameter doivent être en accord
  - DEFAULT: **Accepted** ⇨ **pas de contrôle de l'intégrité**

Client \ Server		CRYPTO_CHECKSUM _SERVER =			
		REJECTED	ACCEPTED	REQUESTED	REQUIRED
CRYPTO_CHECKSUM_CLIENT=	REJECTED	OFF	OFF	OFF Server demande, Client refuse	PAS de Session Server requiert, Client refuse
	ACCEPTED	OFF	OFF Ni le serveur ni le client ne demande!!!	ON Server demande, Client accepte	ON Server demande, Client accepte
	REQUESTED	OFF Client demande, Server refuse	ON Client demande, Server accept	ON Client/Server demandent et acceptent	ON Server requiert, Client demande, les 2 acceptent
	REQUIRED	PAS de Session Client requiert, Server refuse	ON Client requiert, Server accepte	ON Client requiert, Server demande, les 2 acceptent	ON Client et Server requièrent et acceptent

Confidentialité

Oracle 3

Exemple de configuration: sqlnet.ora

- SQLNET.ORA Client (extrait)

```
SQLNET.CRYPTO_CHECKSUM_CLIENT = required
SQLNET.CRYPTO_CHECKSUM_TYPES_CLIENT = (SHA1)
```

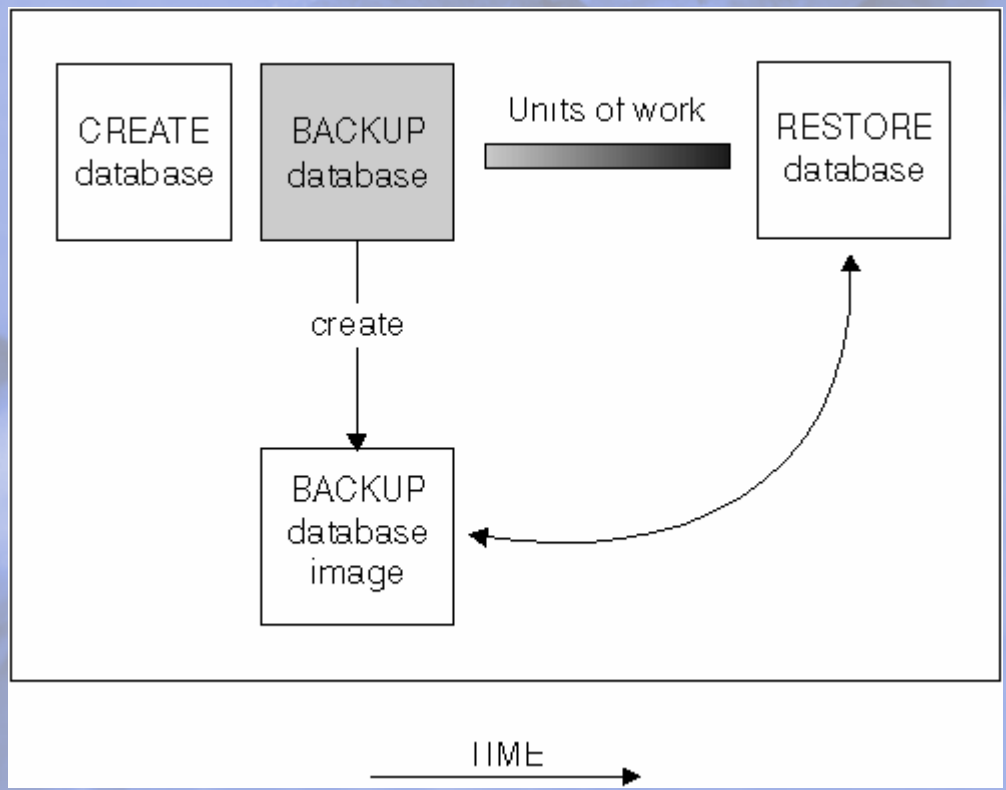
- SQLNET.ORA Server (extrait)

```
SQLNET.CRYPTO_CHECKSUM_SERVER= required
SQLNET.CRYPTO_CHECKSUM_TYPES_SERVER= (SHA1)
```

Disponibilité

DB2 1

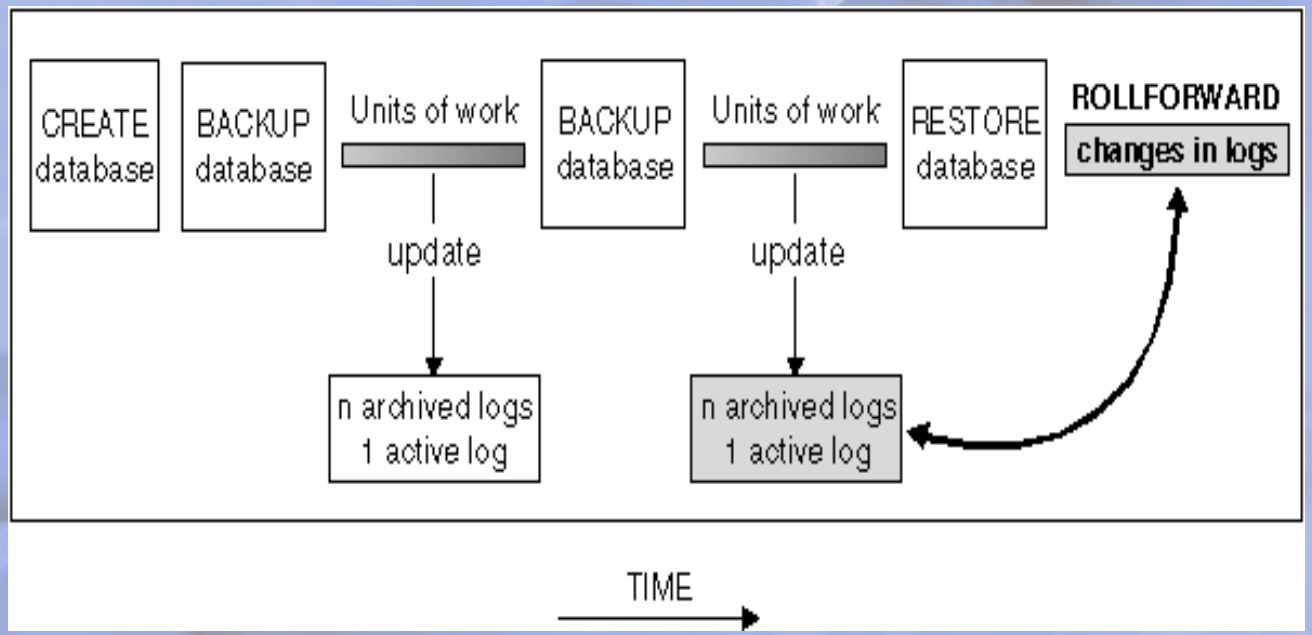
Mode de recouvrement par version



Disponibilité

DB2 2

Mode : «Roll-Forward recovery»



Disponibilité

Oracle 1

Il est possible de faire des copies de sauvegarde via la commande **EXPORT**

ATTENTION, lors de **l'EXPORT,** une transaction non terminé risque de ne pas être sauvegarder adéquatement.

Disponibilité

Oracle 2

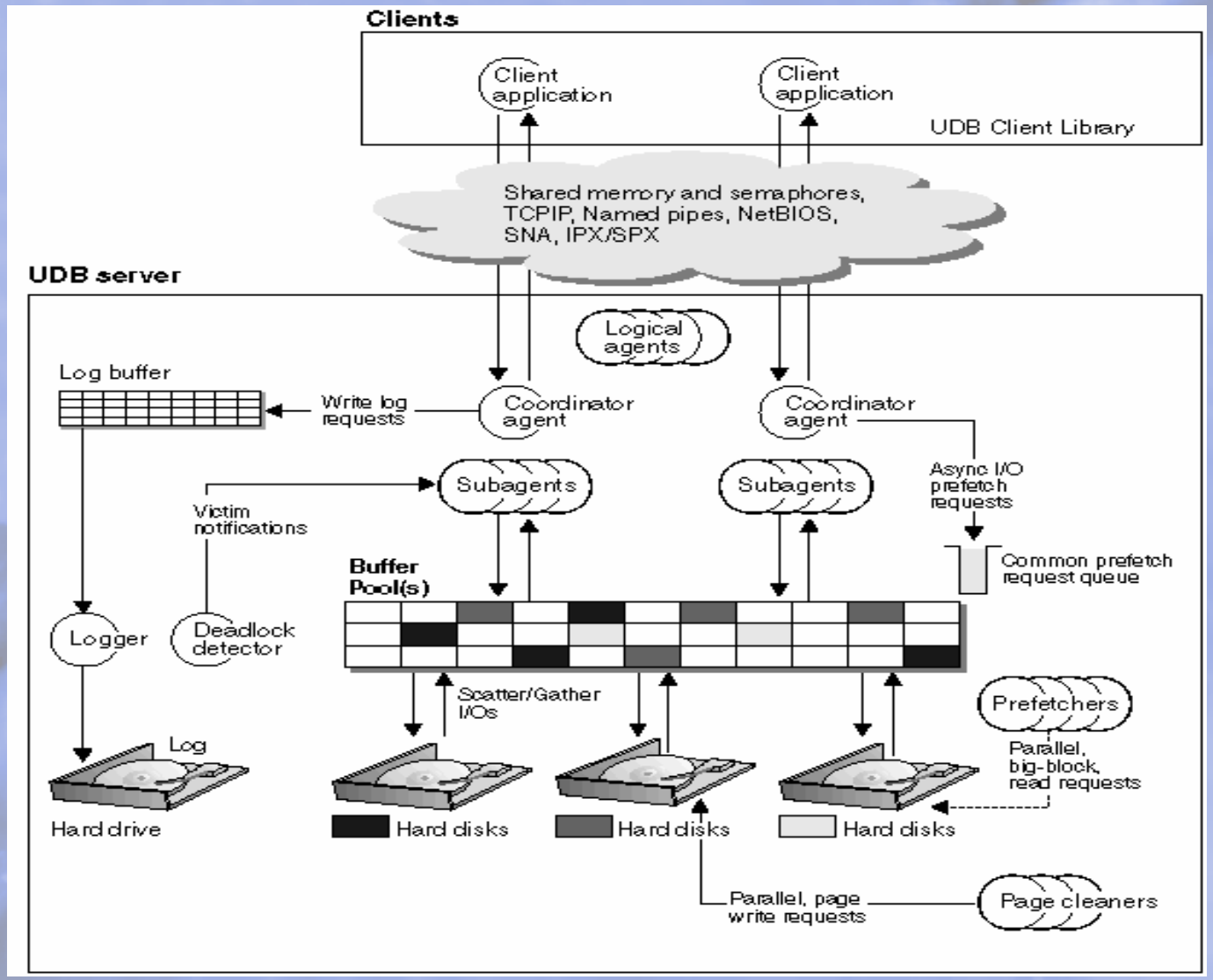
Il existe des mécanismes appelés :

« **Redo LOG** » : Conserve les données jusqu'au COMMIT

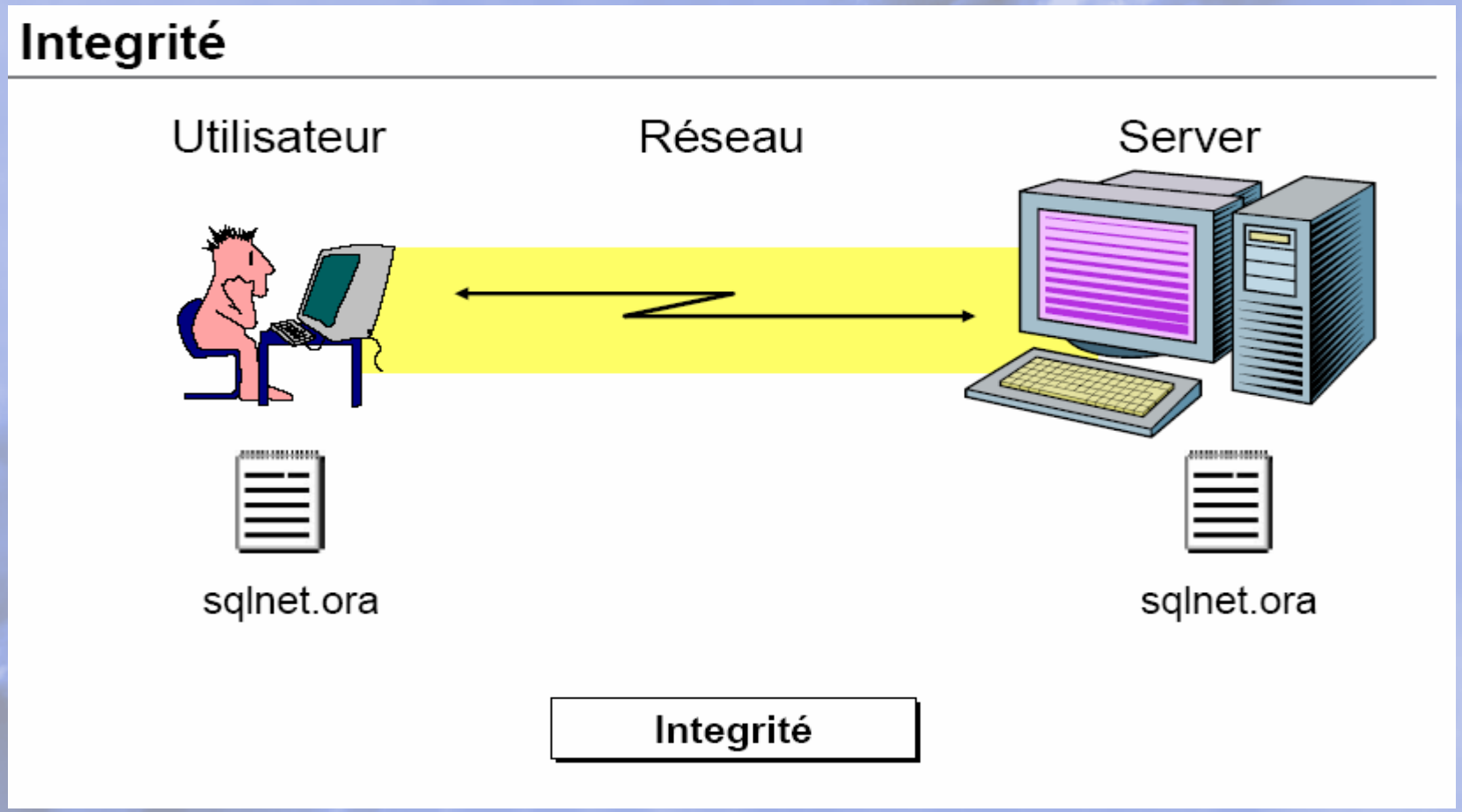
« **RollBack segment** » : Conserve une image des données inchangés jusqu'au COMMIT

Intégrité

DB2



Intégrité


Integrité
Utilisateur
Réseau
Server
sqlnet.ora
sqlnet.ora
Integrité

Intégrité

Oracle 2

Contrôle de l'intégrité

- Le chiffrement à lui seul n'est pas suffisant pour l'intégrité!
- Pour le contrôle d'intégrité Oracle détecte:
  - La modification de paquets de données
  - La perte de paquets de données
  - L'ajout de paquet de données (i.e. Replay Attacks)
- La protection de chaque paquet est faite par:
  - Un numéro de séquence
  - Un checksum (Hash)
  - L'association d'une master clé liée à la session
- Oracle dispose de 2 procédés
  - MD5 Message Digest 5 (128 Bit)
  - SHA-1 Secure Hash Algorithm (160 Bit)

} Checksum faux

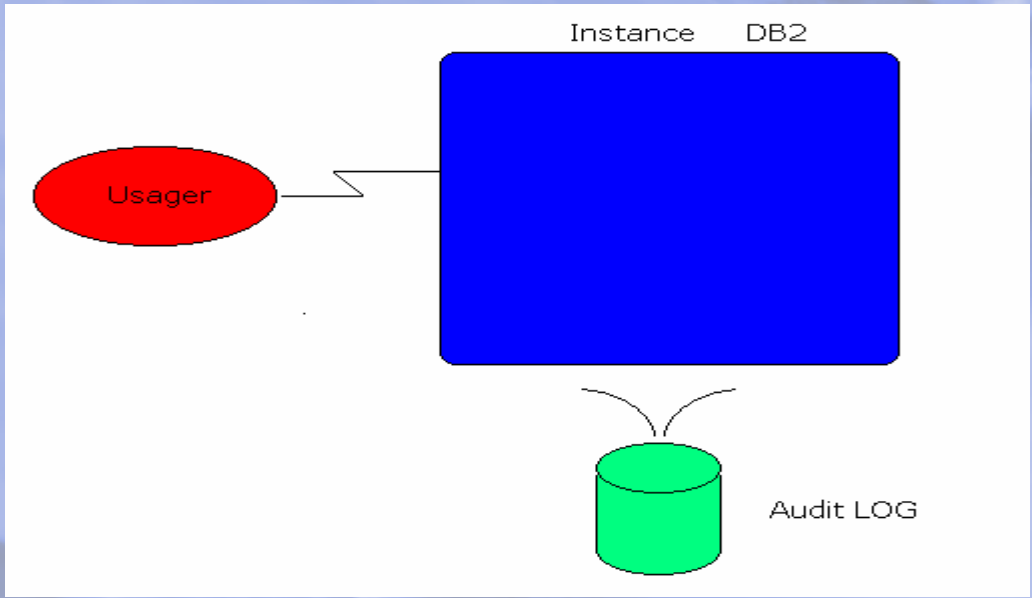
} Numéro de séquence faux

⇩

déconnection

Imputabilité

DB2



DB2AUDIT – permet de formatter et de visualiser le LOGs

Imputabilité

Oracle

Les fonctions d'audits permettent de :

- Surveiller ce qui se passe au niveau logique
  (c'est à dire tous les accès sur les objets et sur les privilèges du système)

- La conservation s'effectue dans une table (SYS.AUDS)
  (sur certains systèmes, il est possible de transférer dans un log système)

- On peut conserver la trace d'une requête, mais non le résultat qui en découle…

En Conclusion

	DB2	Oracle
Authentification	OS	BD OS
Autorisation Privilèges	Structuré et discriminatoire	Structuré et discriminatoire
Confidentialité	À l'interne – Utilise l'OS Lors d'export – selon les besoins	Encodage des informations dans la BD et lors d'exportations (OAS)
Disponibilité	Mécanismes de récupération adéquats.	Mécanismes de récupération adéquats (MAIS – Gestion des transactions non complétées faibles)
Intégrité	Plusieurs mécanismes à divers niveaux sont en place. (SGBD + Réseau)	Plusieurs mécanismes à divers niveaux sont en place. (SGBD)
Imputabilité	Le LOG est conservé dans un fichier séquentiel.	Conserve la trace, mais pas l'information précédente. Le LOG est mise dans une table (SYS.AUDS)n
Donc	Plusieurs fonctions décentralisés	Tout est centralisé

Questions?