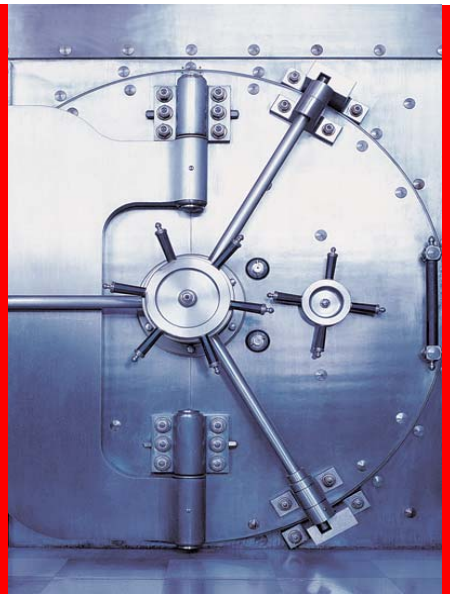


ORACLE

Sécuriser les bases de données ORACLE

Michel PIGNATA
Consultant-Vente Solutions Technologiques
Jean-Philippe PINTE
Consultant-Vente Solutions Technologiques

Juillet 2008

Agenda

- Sécurité des données
  les enjeux pour l'entreprise

- Oracle DatabaseVault, Oracle Audit Vault, Oracle Total Recall
  Faciliter la mise en conformité réglementaire sans
  modification applicative
  Démonstration

Oracle Advanced Security et Oracle Label Security
  Conformité réglementaire pour une protection tournée
  vers l'interne comme vers l'extérieur de l'entreprise
  Démonstration

- Oracle Data Masking
  Comment protéger ses données confidentielles en phase de test ?
  Démonstration

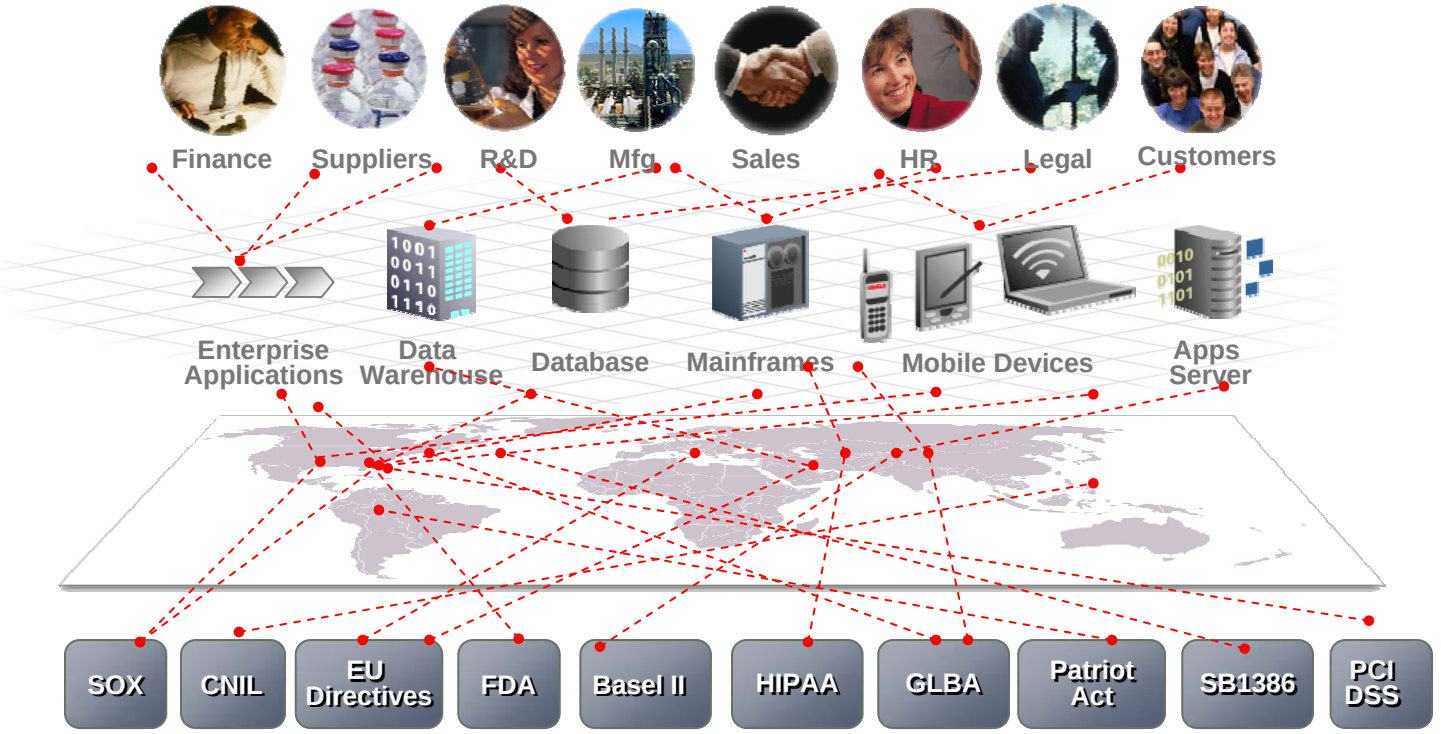
Sécurité des données

Une prise de conscience grandissante

- La sécurité de l'information est vitale. Elle conditionne l'activité économique des entreprises et la confiance dans les organismes publics
- La divulgation volontaire ou accidentelle de données financières ou privées peut avoir des conséquences fâcheuses sur le plan
  - Economique, commercial et…juridique
- 25 % des incidents sont le fait de personnels internes
- 50 % sont consécutifs à des pertes ou des vols de matériels divers

GRC: Le nouveau Graal

Gouvernance, risques, conformité



Quelques unes des réglementations apparues ces dernières années…

Sécurité des SI
Une affaire de risques

- L ’analyse des risques conduit généralement à considérer 5 objectifs de sécurité de l’information
  - Sa **confidentialité**
  - Son **intégrité**
  - Son utilisation **conforme** aux règles
  - Sa **disponibilité**
  - La **traçabilité** de son utilisation

Sécurité des SI

Confidentialité

- Empêcher la consultation de données sensibles par des personnes non autorisées
  - Qui a accès?
  - Quels sont les mécanismes de contrôle d'accès ?
  - Quid des utilisateurs à super privilèges ?
  - Les données sont-elles protégées par du chiffrement:
    - Lors de leur stockage ?
    - Durant leurs mouvements ?
  - …

Sécurité des SI

Intégrité

- Prévenir la modification des données par des personnes non autorisées
  - Qui peut modifier l'information ?
  - Quels contrôles sont en place pour limiter les accès ? Pour donner les accès ?
  - Quels sont les mécanismes permettant de vérifier si l'information a été changée ?
  - Quels moyens sont utilisés par les applications pour contrôler la cohérence des informations ?
  - …

Sécurité des SI

Traçabilité / Conformité

- Permettre de garder la trace des actions effectuées sur les systèmes, à des fins de prévention, de dissuasion et d'audit des incidents
  - Qui a accédé ?
  - Quelle information sur l'activité est capturée ?
  - Comment sont protégés les référentiels d'audit ?
  - Une exploitation systématique des audits est-elle en place ?
  - …

Sécurité des bases Oracle

Une constante innovation

Oracle Database 11g

Data Masking

TDE Tablespace Encryption

Oracle Total Recall

Oracle Database 10g

Oracle Audit Vault

Oracle Database Vault

Transparent Data Encryption (TDE)

Real Time Masking

Oracle Database 9i

Secure Config Scanning

Fine Grained Auditing

Oracle Label Security

Enterprise User Security

Oracle8i

Virtual Private Database (VPD)

Database Encryption API

Strong Authentication

Native Network Encryption

Oracle7

Database Auditing

Government customer

Confidentialité des données et Conformité Réglementaire

Les Défis de la sécurité Base De Données

Contrôles d'Accès

Surveillance

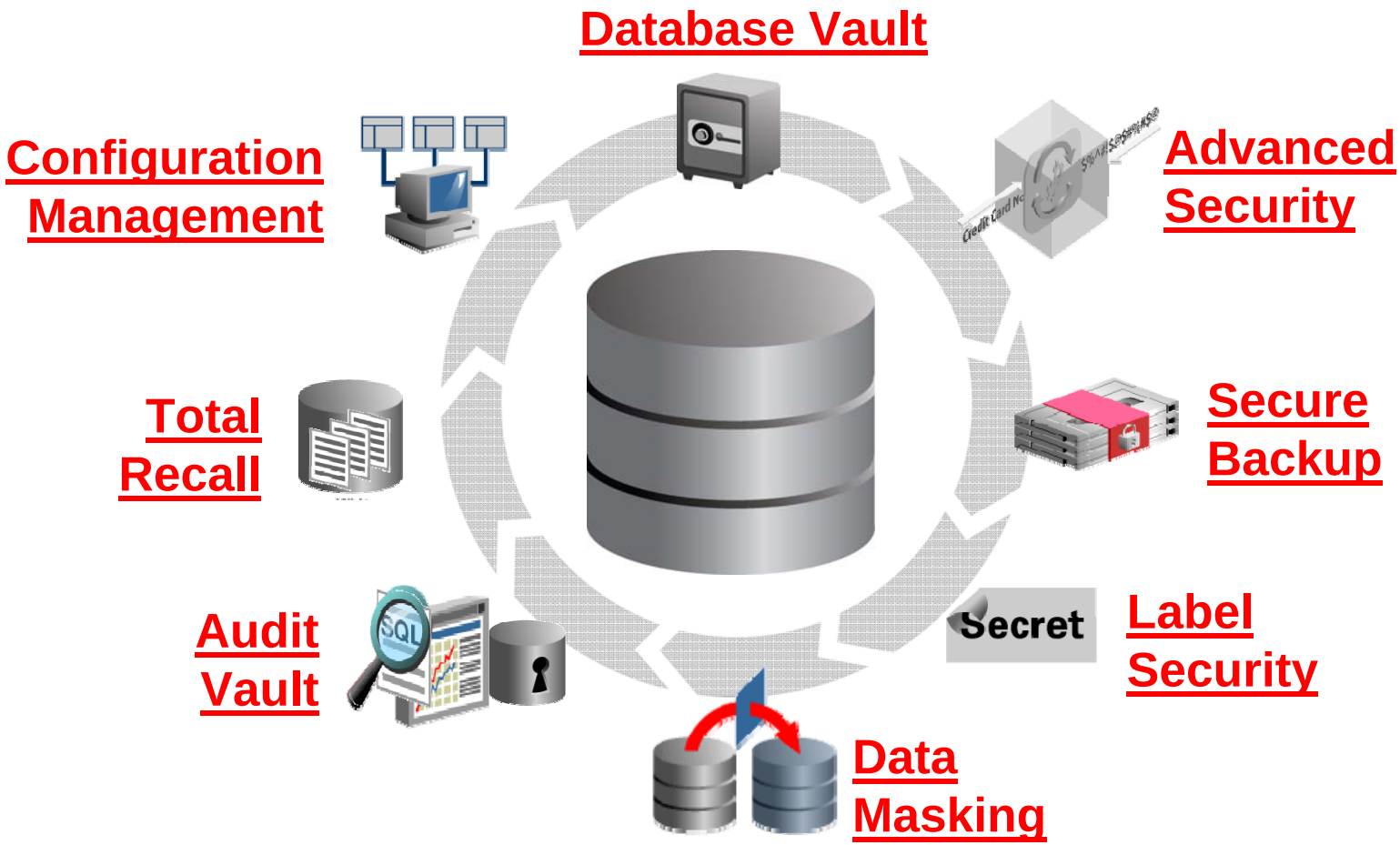
Protection des données

De-Identification des données pour partage

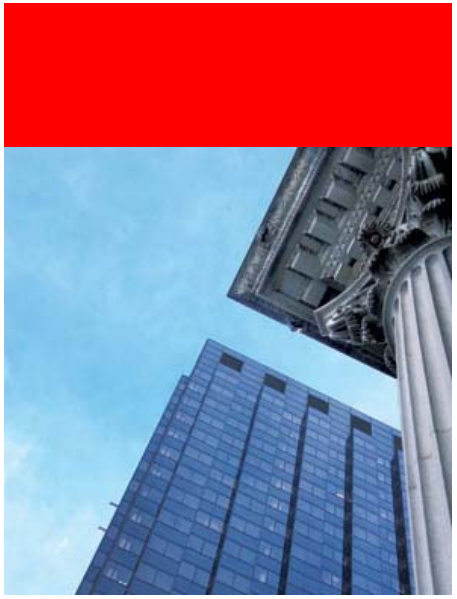
Classification des données

Oracle Database Security

Solutions pour la confidentialité et la conformité



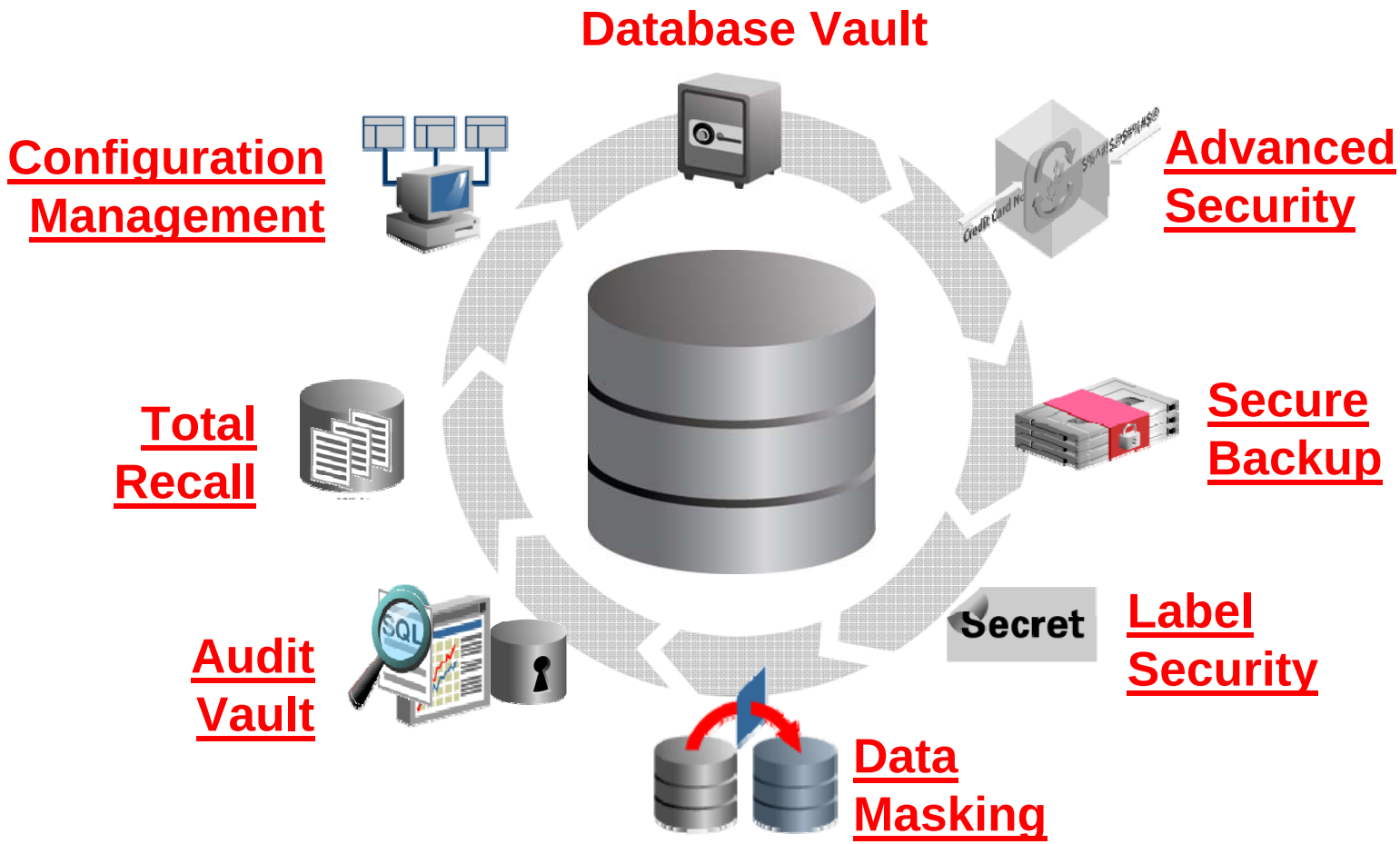
Faciliter la mise en conformité réglementaire sans modification applicative



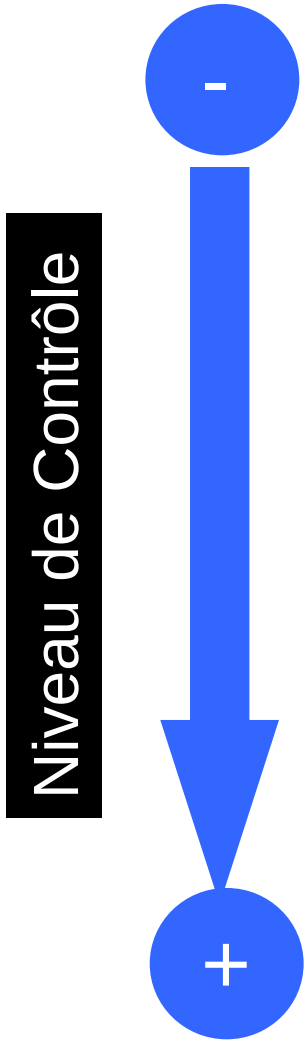
- Oracle Database Vault
- Oracle Audit Vault
- Oracle Total Recall

Oracle Database Security

Solutions pour la confidentialité et la conformité



Les Contrôles d'accès



- Discretionary Access Control (DAC)
- Secure Application Role (SAR)
- Virtual Private database (VPD)
- Oracle Label Security (LBAC)

Privilèges spéciaux

- Database Vault

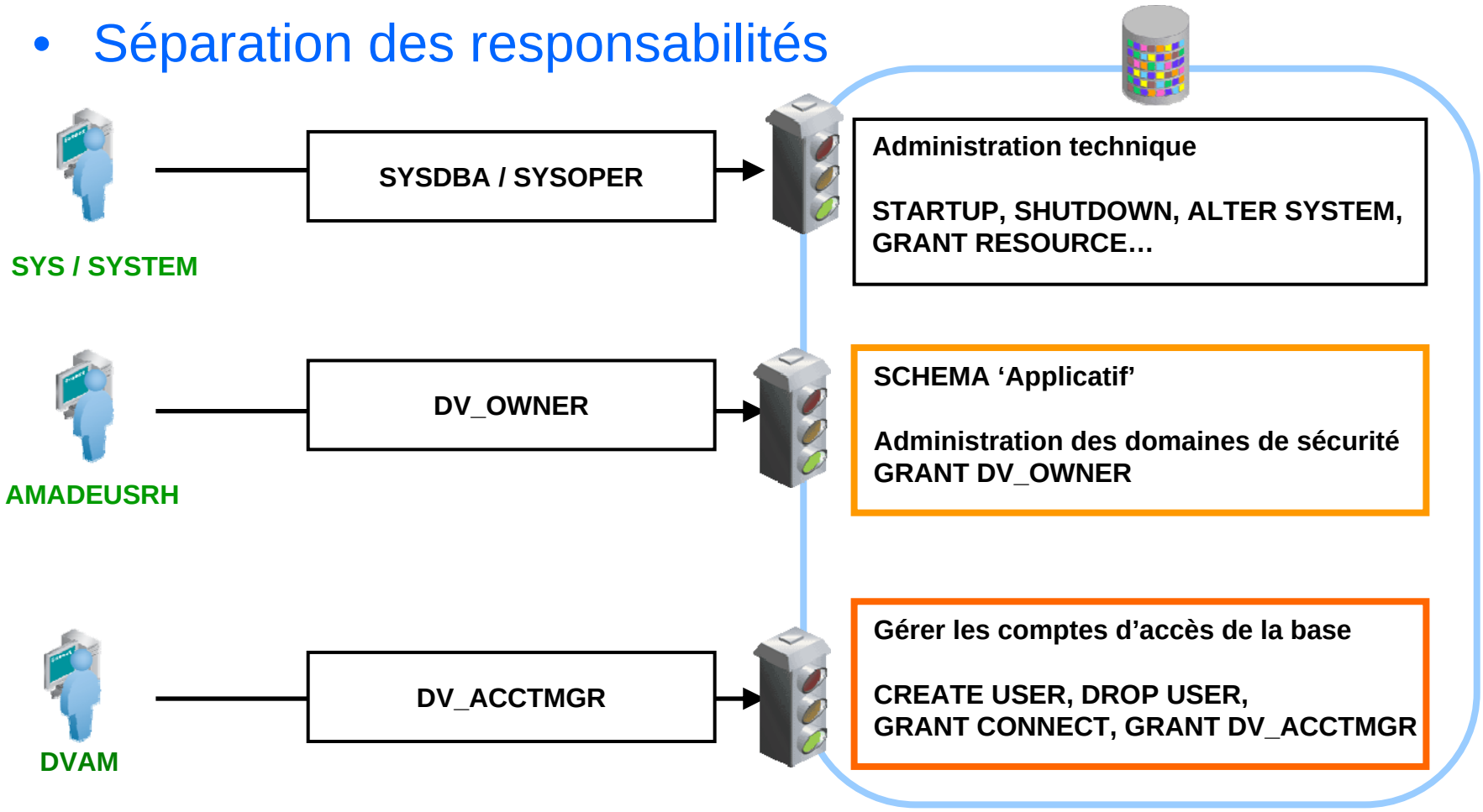
Privilèges spéciaux

Oracle Database Vault

- Pourquoi faire ?
  - Protéger les données des accès par les personnes disposant de privilèges exceptionnels
  - …et n'ayant pas de droits d'accès octroyés par leur fonction dans l'entreprise
- Bénéfices attendus
  - Permettre aux responsables d'application de prendre des engagements quant à la sécurité de leurs données
  - Garantir une séparation stricte des responsabilités

Privilèges spéciaux
Oracle Database Vault

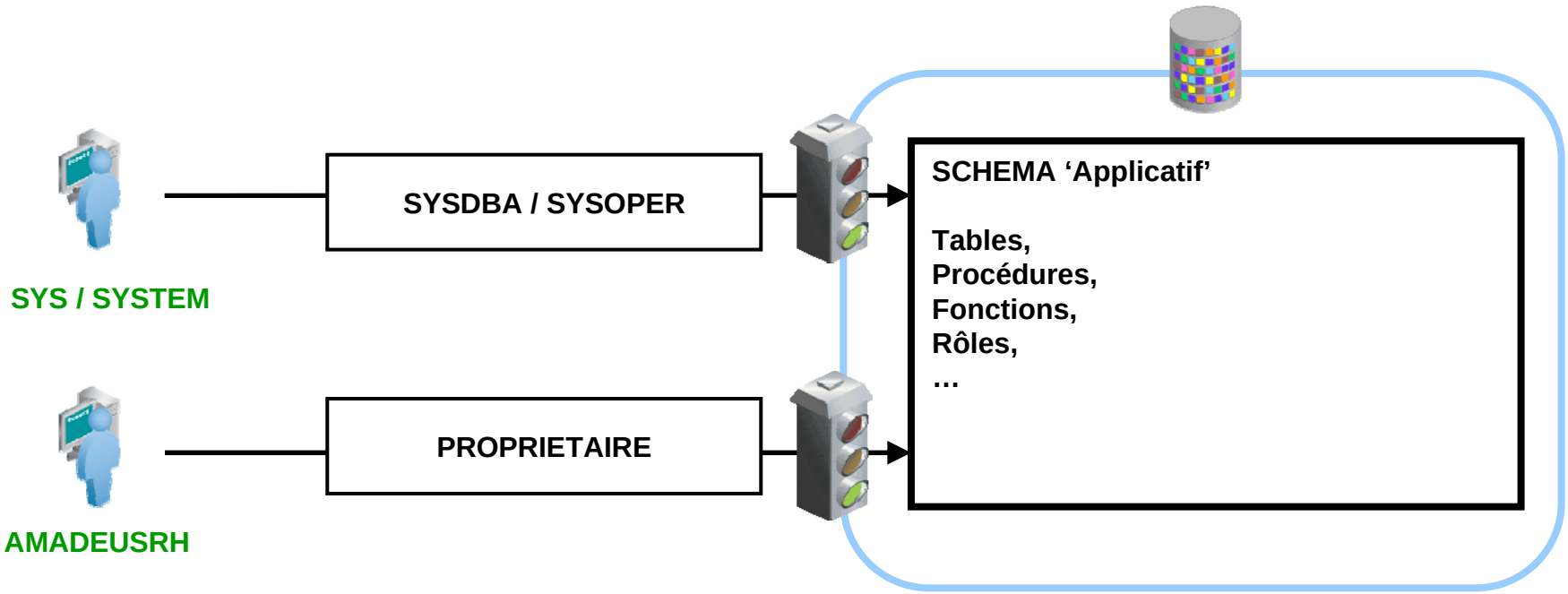
- Séparation des responsabilités



Privilèges spéciaux

Oracle Database Vault

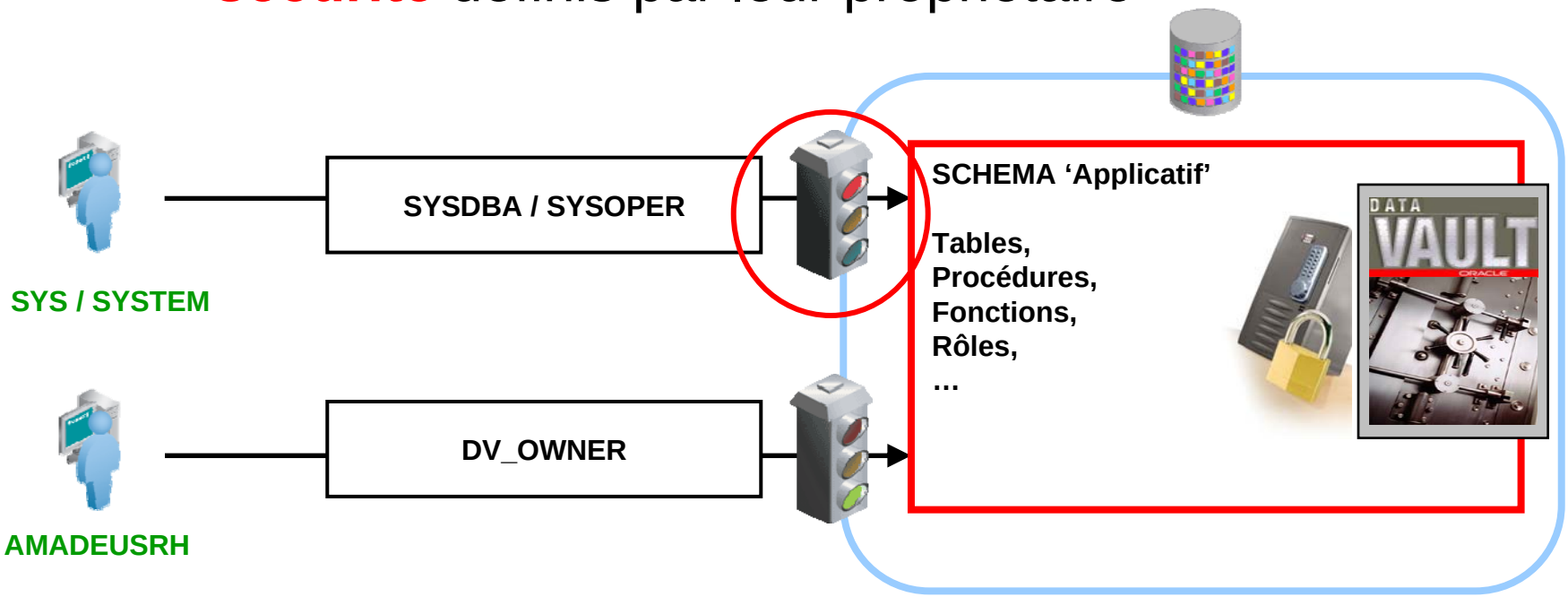
- Protection des utilisateurs à forts privilèges



Privilèges spéciaux

Oracle Database Vault

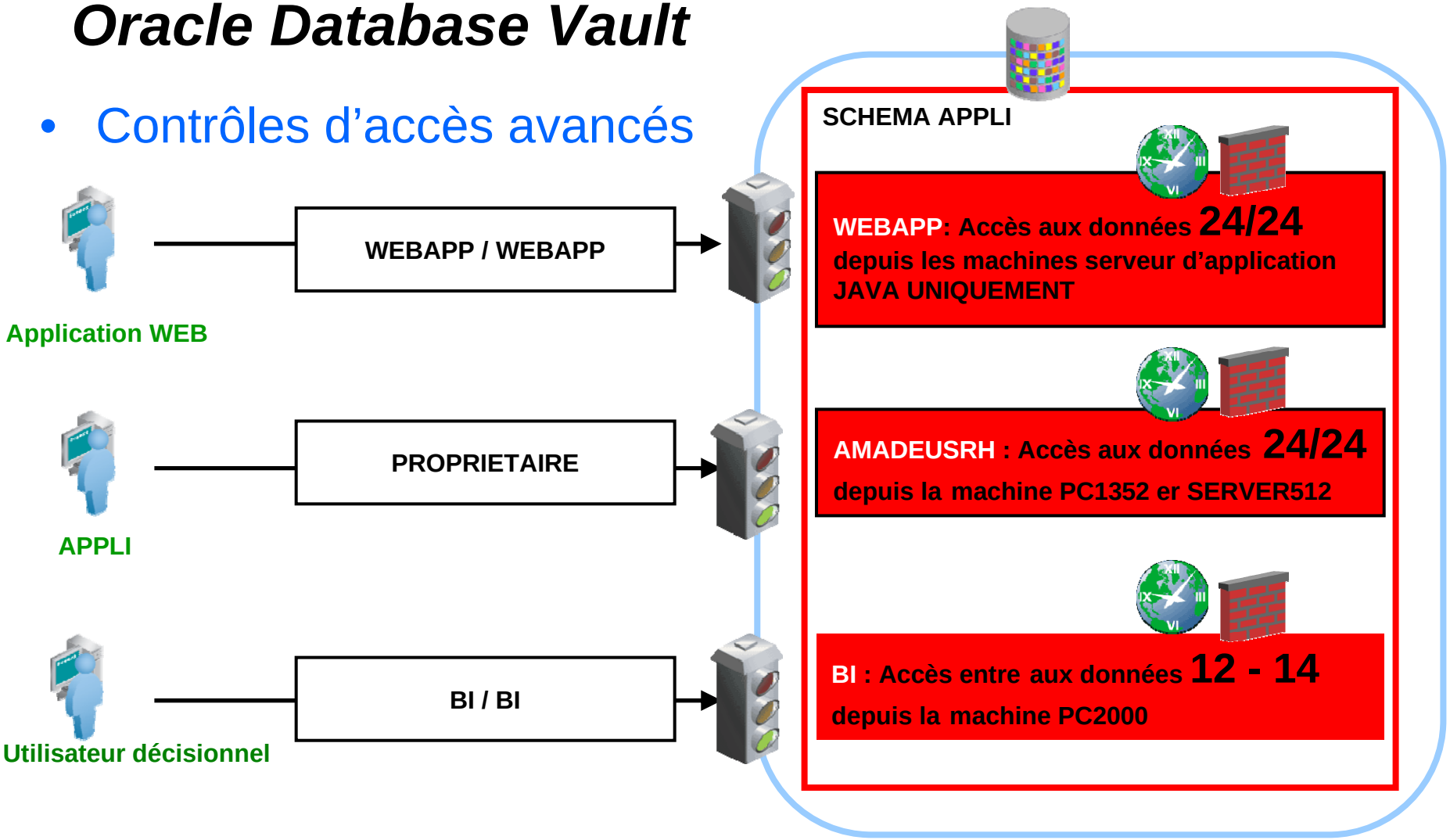
- Protection des utilisateurs à forts privilèges
  - Les données sont protégées par des **domaines de sécurité** définis par leur propriétaire



Privilèges spéciaux

Oracle Database Vault

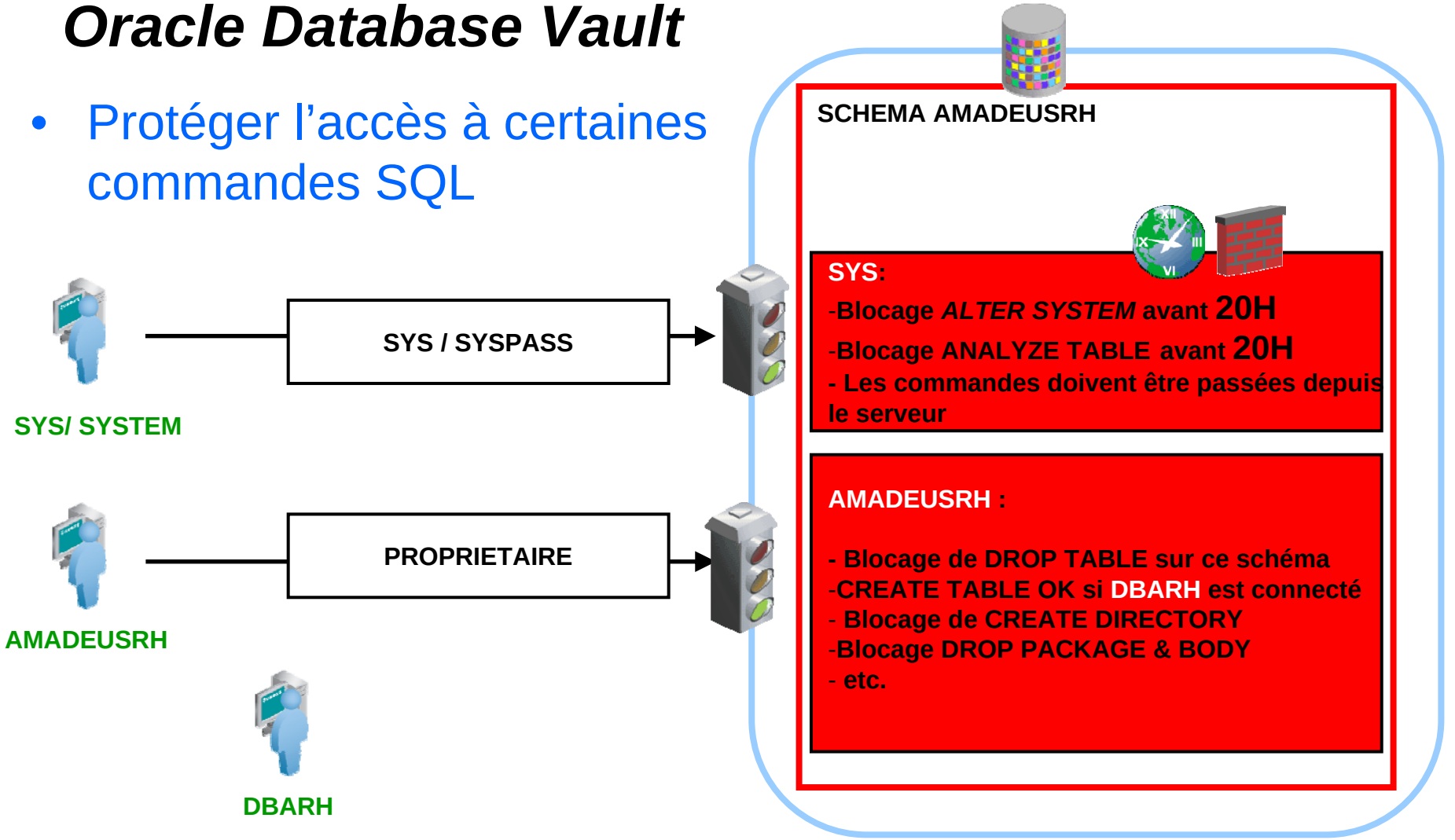
- Contrôles d'accès avancés



Privilèges spéciaux

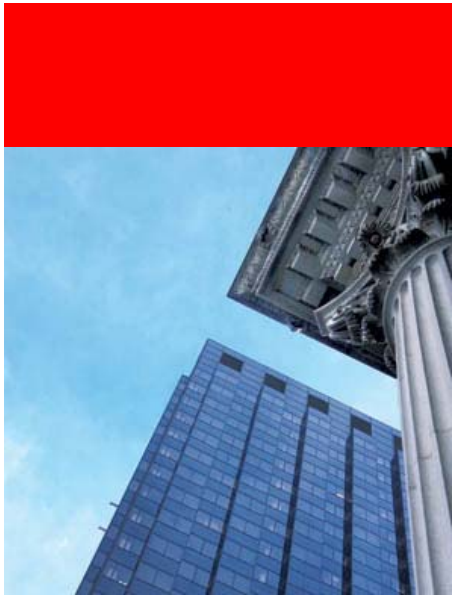
Oracle Database Vault

- Protéger l'accès à certaines commandes SQL



Privilèges spéciaux
Oracle Database Vault

- Audit
  - En succès, en échec ou les deux
  - Des politiques de protection définies sur
    - les tables, les vues
    - les séquences
    - les procédures et les fonctions PL/SQL, les rôles, etc.
  - Des tentatives accordées ou rejetées d'utilisation de commandes SQL protégées



Démonstration

Oracle Database Vault

Auditer des bases

Oracle Audit Vault

- Pourquoi faire ?
  - Garder la trace de certaines actions effectuées sur les bases de données
- Bénéfices attendus
  - Progressivement mettre en place une architecture solide de règles d'audit des bases
  - Collecter systématiquement en lieu sûr, les évènements produits par les sources d'audit
  - Analyser les évènements remontés
  - Faciliter la gestion du cycle de vie des données d'audit

Auditer des bases

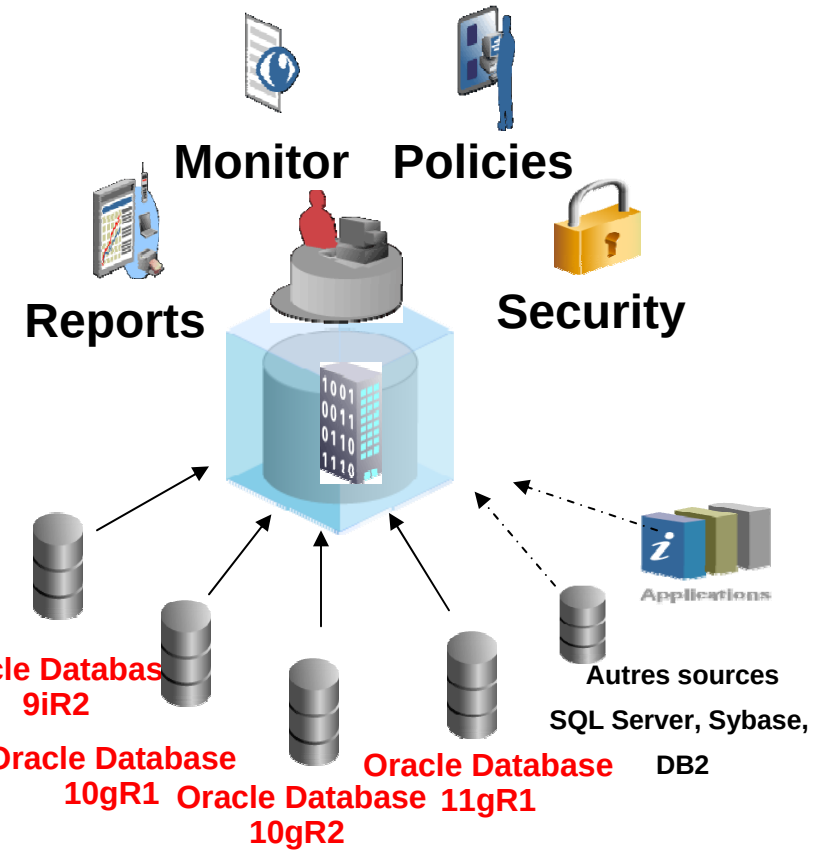
Oracle Audit

- Deux types d'audit existent
  - Standard. Pour auditer tout ce qui peut s'imaginer! Les ordres DDL et DML. A privilégier pour tout ce qui est DDL et utilisation de privilèges
  - '*Fine Grained*'. Permet de réduire la volumétrie de l'audit en ciblant les conditions de déclenchement sur des conditions précises
- Ou stocker l'audit?
  - Dans la base cible ou sur des fichiers externes

Auditer des bases

Oracle Audit Vault

- Collecte & Consolidation les données d'Audit
  - Oracle 9i Release 2 et postérieures
  - Autres SGBD (SQLServer, Sybase, DB2)
- Définition des politiques d'Audit sur les bases cibles dans un référentiel central
- Provisionning des politiques d'Audit vers les cibles
- Comparaison des politiques mises en place vis-à-vis du référentiel
- Simplification du reporting pour conformité
  - Etats prédéfinis
  - Etats personnalisables
- Détecte et prévient les menaces internes
  - Alertes d'Activité suspectes



Audit Vault Reports

Evaluations d'Audit & Etats personnalisés

- Etats prédéfinis
  - Activité des utilisateurs privilégiés
  - Accès à des données sensibles
  - Attribution de droits à des rôles
  - Activité DDL
  - Login/logout
- Etats liés aux utilisateurs
  - Quels utilisateurs privilégiés accèdent aux données financières ?
  - Quelles données peuvent être accédées par un user 'A' dans différentes base de données ?
  - Qui accède à des données sensibles ?
- Etats personnalisés
  - Oracle BI Publisher, Application Express, Outils Tiers


ORACLE Enterprise Manager 10g
Audit Vault

Overview | Activity Reports | Alert Report

Database Instance: av > Privileged Users Activity - Past 24 Hours: JTAYLOR, SYSTEM, SYS

Privileged Users Activity - Past 24 Hours: JTAYLOR, SYSTEM, SYS

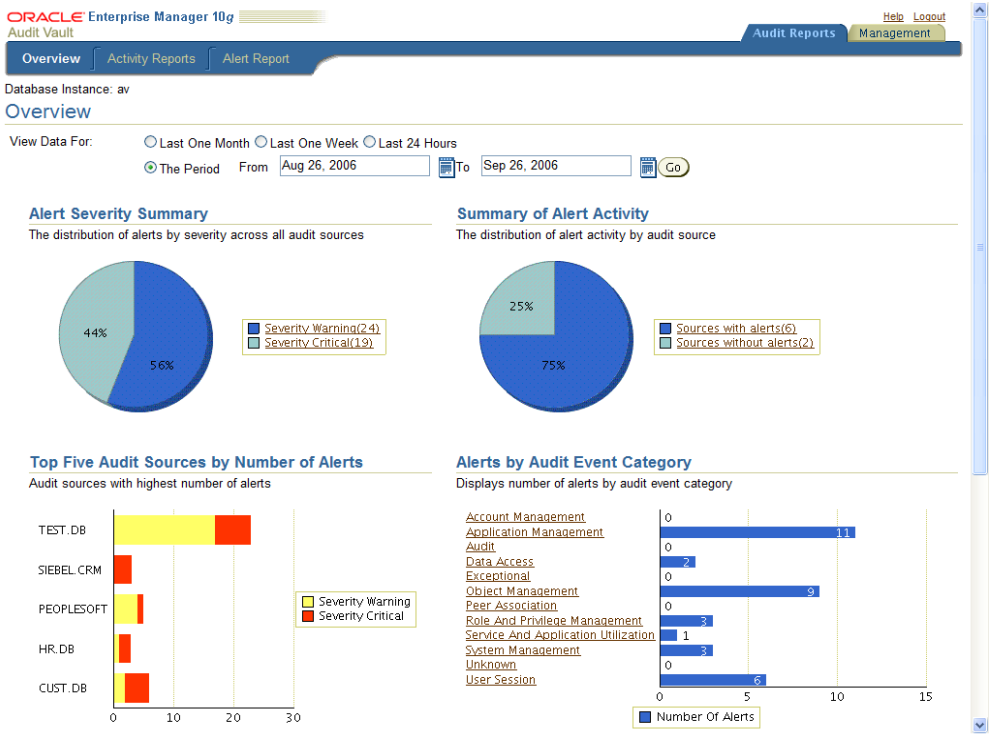
Privileged user activity over the past 24 hours: JTAYLOR, SYSTEM, SYS

Audit Source	User	Audit Event Category	Audit Event	Object	Client Host
VMSSRC2.ORACLE.COM	JTAYLOR	OBJECT MANAGEMENT	DROP TABLE	SCOTT.EMP1	vipshah-lap2
VMSSRC2.ORACLE.COM	JTAYLOR	OBJECT MANAGEMENT	DROP TABLE	SCOTT.EMP2	vipshah-lap2
VMSSRC2.ORACLE.COM	JTAYLOR	OBJECT MANAGEMENT	CREATE TABLE	SCOTT.EMP2	vipshah-lap2
VMSSRC2.ORACLE.COM	JTAYLOR	OBJECT MANAGEMENT	CREATE TABLE	SCOTT.EMP1	vipshah-lap2
VMSSRC2.ORACLE.COM	JTAYLOR	OBJECT MANAGEMENT	ALTER TABLE	SCOTT.EMP1	vipshah-lap2
VMSSRC2.ORACLE.COM	JTAYLOR	OBJECT MANAGEMENT	ALTER TABLE	JTAYLOR.EMP1	vipshah-lap2
VMSSRC2.ORACLE.COM	JTAYLOR	OBJECT MANAGEMENT	CREATE TABLE	SCOTT.EMP1	vipshah-lap2
VMSSRC2.ORACLE.COM	JTAYLOR	OBJECT MANAGEMENT	DROP TABLE	SCOTT.EMP1	vipshah-lap2
VMSSRC2.ORACLE.COM	JTAYLOR	USER SESSION	LOGON		vipshah-lap2
ORCL.US.ORACLE.COM	JTAYLOR	DATA ACCESS	SELECT	SH.SALES	raclinux1.us.oracle.com
ORCL.US.ORACLE.COM	JTAYLOR	USER SESSION	LOGON		raclinux1.us.oracle.com
VMSSRC2.ORACLE.COM	SYS	USER SESSION	LOGON		vipshah-lap2
ORCL.US.ORACLE.COM	sys	USER SESSION	SUPER USER LOGON		
ORCL.US.ORACLE.COM	/	USER SESSION	SUPER USER		

Oracle Audit Vault

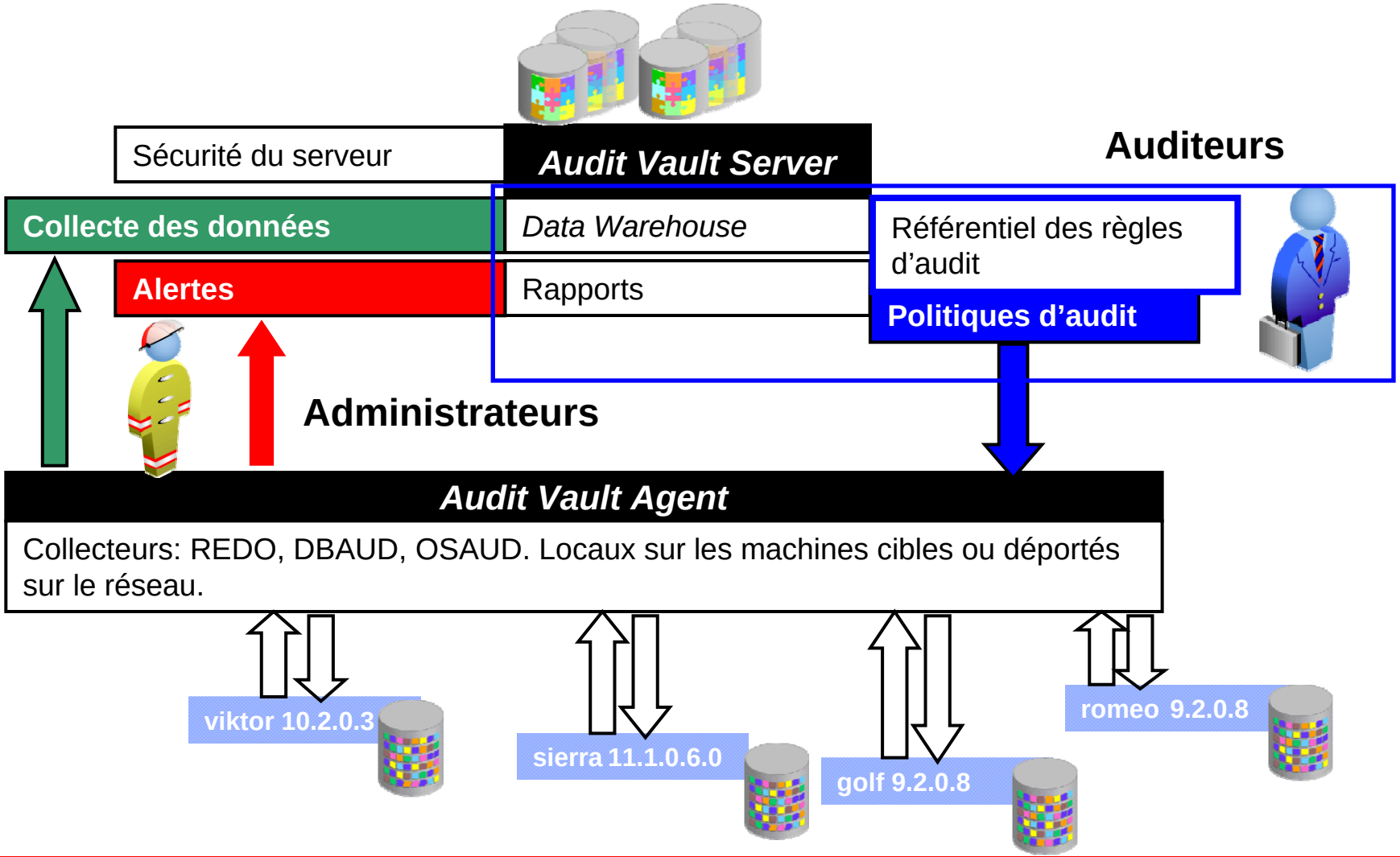
Administration

- Tableau de bord Audit Vault
  - VueEnterprise
  - Alertes et Etats
  - Administration
  - Politiques d'Audit
- Politiques Audit Vault
  - Centralise les paramètres d'audit pour les politiques de conformité
  - Collecte des paramètres d'audit des bases de données
  - Comparaison avec les paramètres d'audits des sources
  - Demonstration de la conformité



Oracle Audit Vault

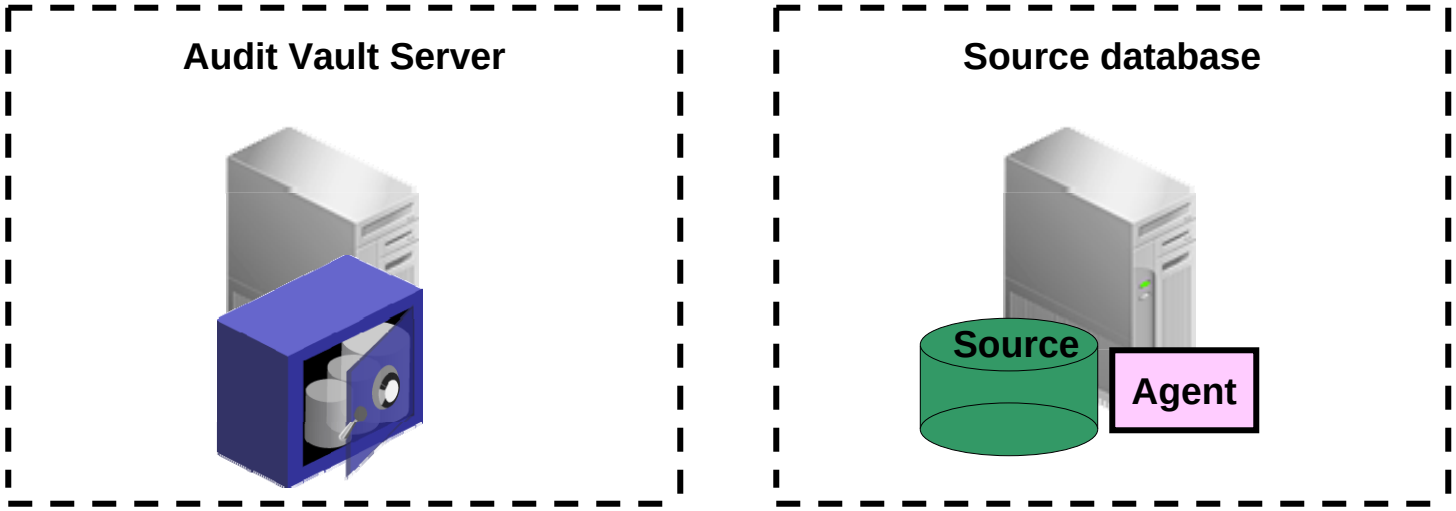
Architecture



Oracle Audit Vault

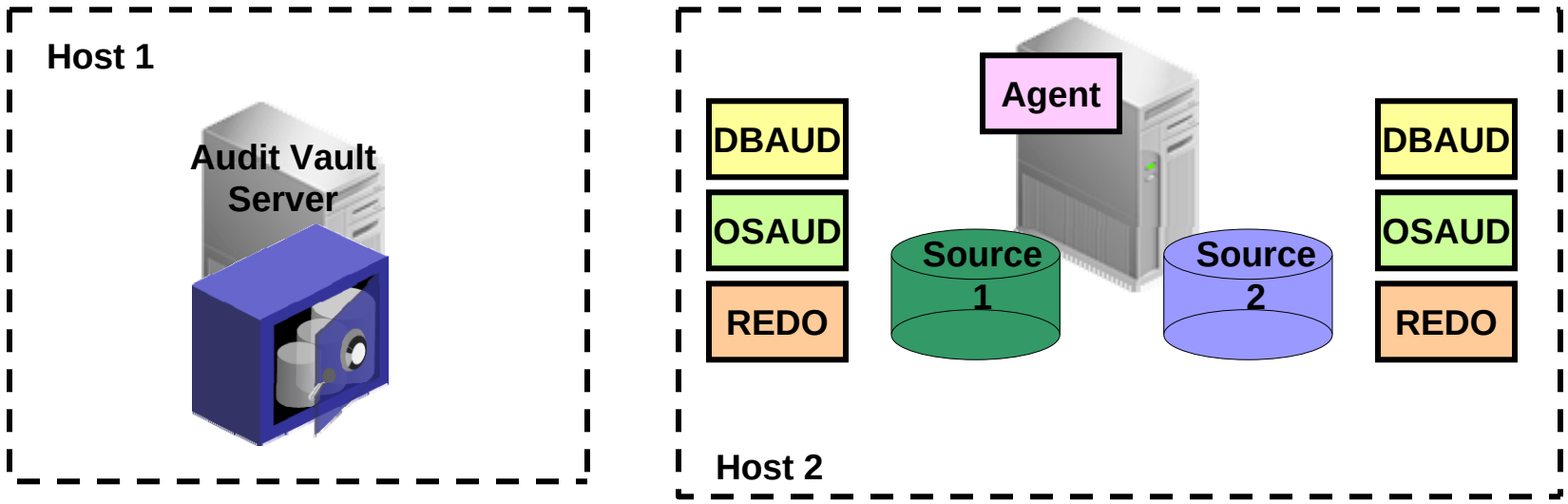
Déploiement

- Le serveur *Audit Vault* est installé sur un environnement dédié



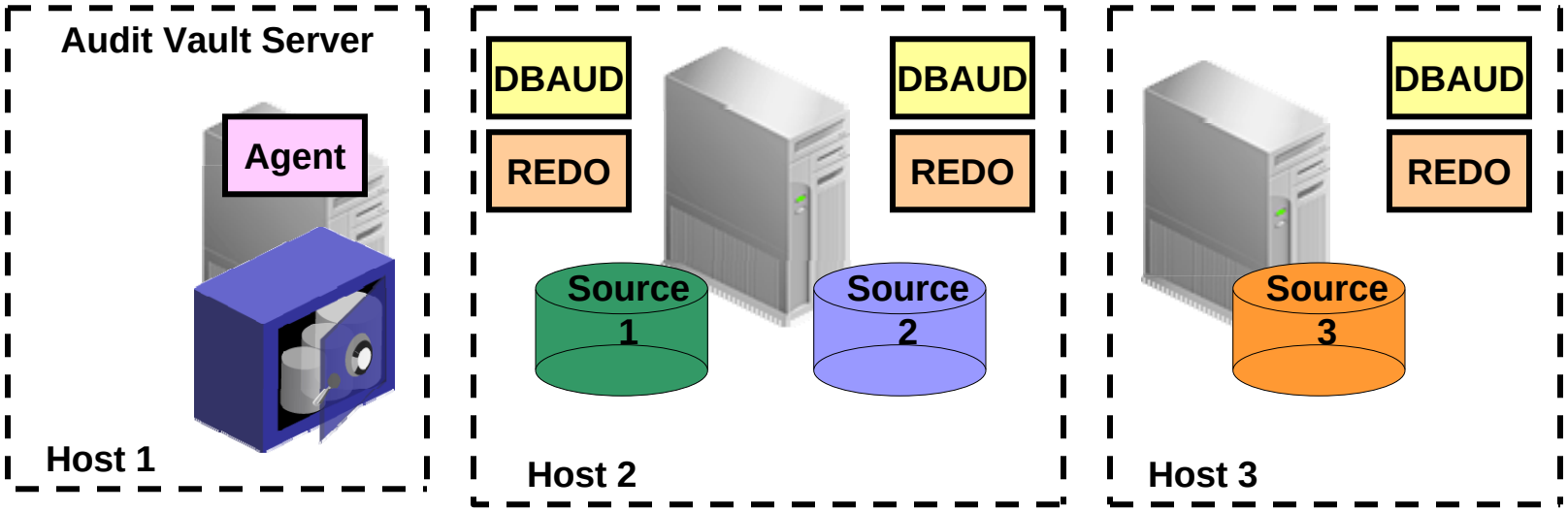
Oracle Audit Vault
Déploiement

- L'*Audit Vault Collection Agent* peut être installé sur la machine où est la base cible
- Un agent peut supporter plusieurs sources d'audit (bases)



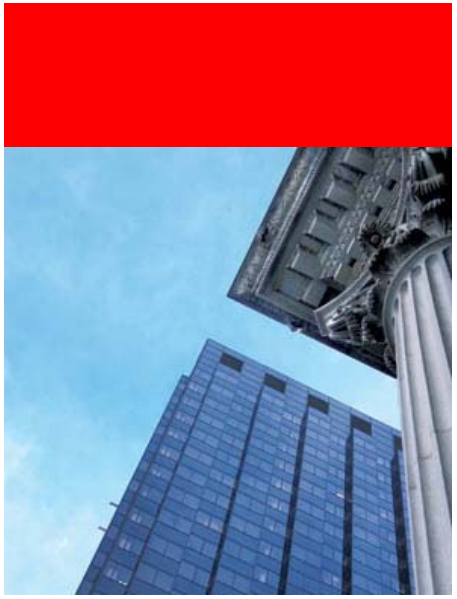
Oracle Audit Vault
Déploiement

- L'*Audit Vault Collection Agent* peut aussi être installé sur d'autres machines que les bases
- Mais ce modèle de déploiement ne supporte que les collecteurs DBAUD et REDO



Oracle Audit Vault
Déploiement

- *Audit Vault* est livré avec un modèle décisionnel (*star schema*)
  - La table des faits rafraichie par défaut toutes les 24H, collecte les évènements d'audit
  - 9 dimensions permettent des analyses par
    - Type d'évènement
    - Chronologie
    - Source d'audit
    - Utilisation de privilèges
    - Clients des bases
    - Utilisateurs, etc.



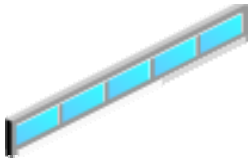
Démonstration

Oracle Audit Vault

Oracle Total Recall

Flashback Data Archive

ORACLE 11g DATABASE



Flashback Query

ORACLE 9i INTERNET

Flashback Tables

ORACLE 10g DATABASE

Flashback Database

ORACLE 10g DATABASE

Flashback Data Archive

ORACLE 11g DATABASE

Flashback Data Archive

- L'archivage des données sensibles et l'historique de leurs évolutions dans des TABLESPACES dédiés (ou non) est automatisable
- Plus de dépendance vis-à-vis des UNDO comme en 9i et 10g

```
CREATE FLASHBACK ARCHIVE UNMOIS
       TABLESPACE TBS_UNMOIS
       RETENTION 1 MONTH;
```

```
ALTER TABLE PEOPLE FLASHBACK ARCHIVE UNMOIS;
```

Flashback Data Archive

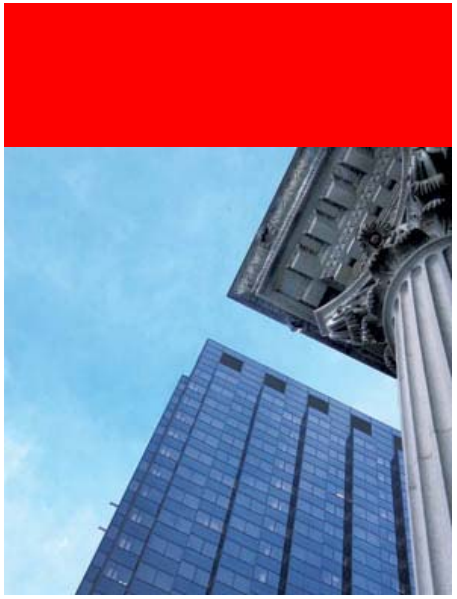
- On peut ainsi créer des espaces d'archivage avec des périodes de rétention différentes
- Puis attacher les tables concernées à ces espaces d'archivage
- La base maintiendra ces historiques de données. La capture des changements est automatique et asynchrone (*process* spécialisé)
- Les données archivées sont compressées systématiquement
- Elles sont accessibles avec la syntaxe:

```
select upper(peo_lastname), peo_salary, p.job_id, job_label
   from people P, jobs J
   as of timestamp to_timestamp ('12/31/2003 12:39:00','mm/dd/yyyy hh24:mi:ss')
   where … P.job_id = J.job_id order by peo_lastname  asc;
```

Flashback Data Archive

- FDA permet, par sa simplicité de mise en œuvre la mise en place rapide d'un archivage de l'historique des données
  - Processus et stockage dédié pour assurer un impact faible sur les performances
  - Rétention automatique sur une période de temps définie
  - Assure une capacité d'analyse à postériori des évolutions de la donnée
  - Permet l'éventuelle correction d'erreurs ou de malversations

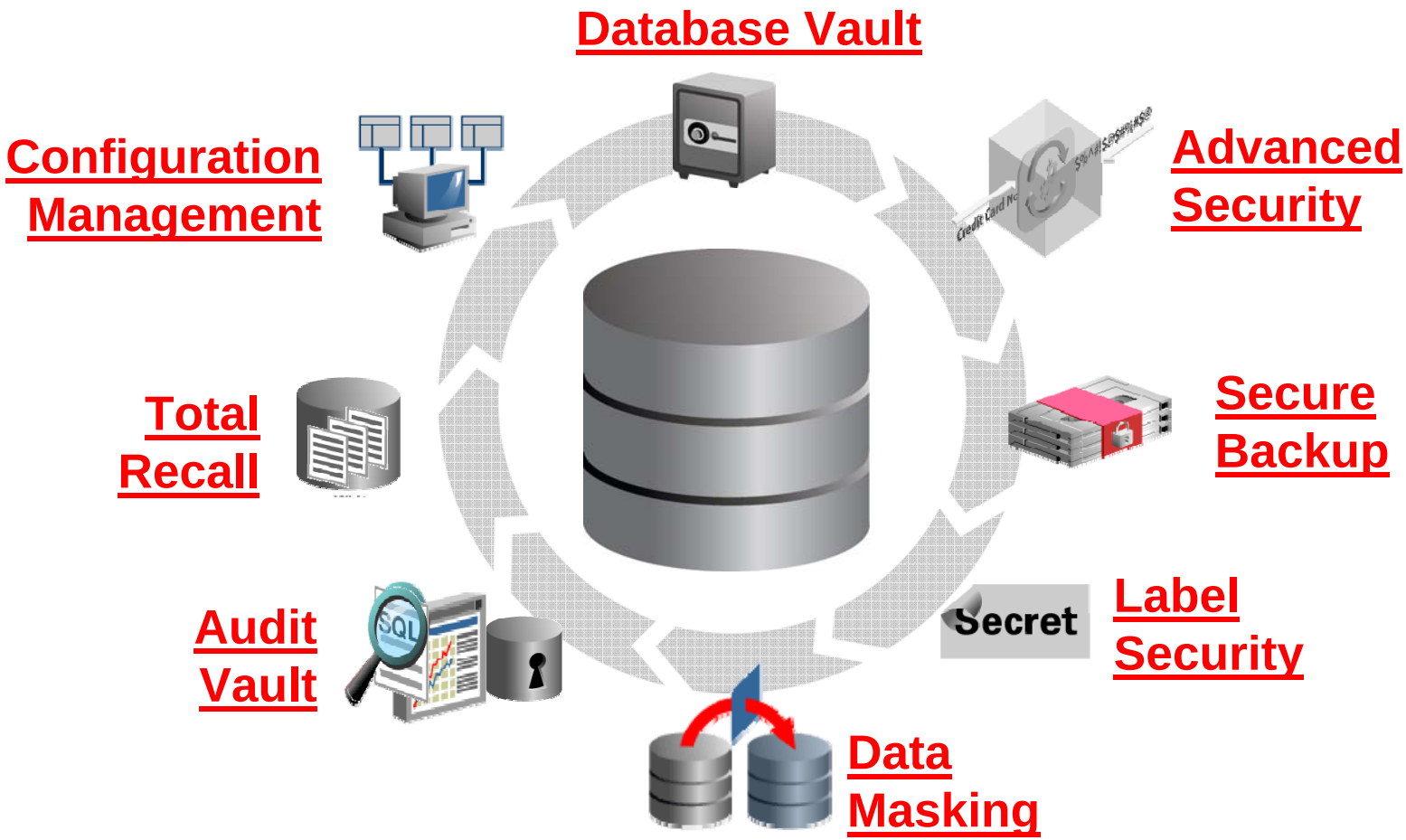
Conformité réglementaire pour une protecion tournée vers l'interne comme vers l'extérieur de l'entreprise



- Oracle Advanced Security
- Oracle Secure Backup
- Oracle Label Security

Oracle Database Security

Solutions pour la confidentialité et la conformité

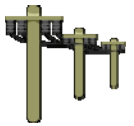


Chiffrement

Advanced Security Option

- Pourquoi faire ?
  - Protéger les données lors de leur transport
  - Protéger les données lors de leur stockage
- Bénéfices attendus
  - Assurer la protection contre des attaques physiques sur les fichiers
  - Protéger les flux réseau
  - Se couvrir de la perte ou du vol de supports physiques

Chiffrement
OracleNet

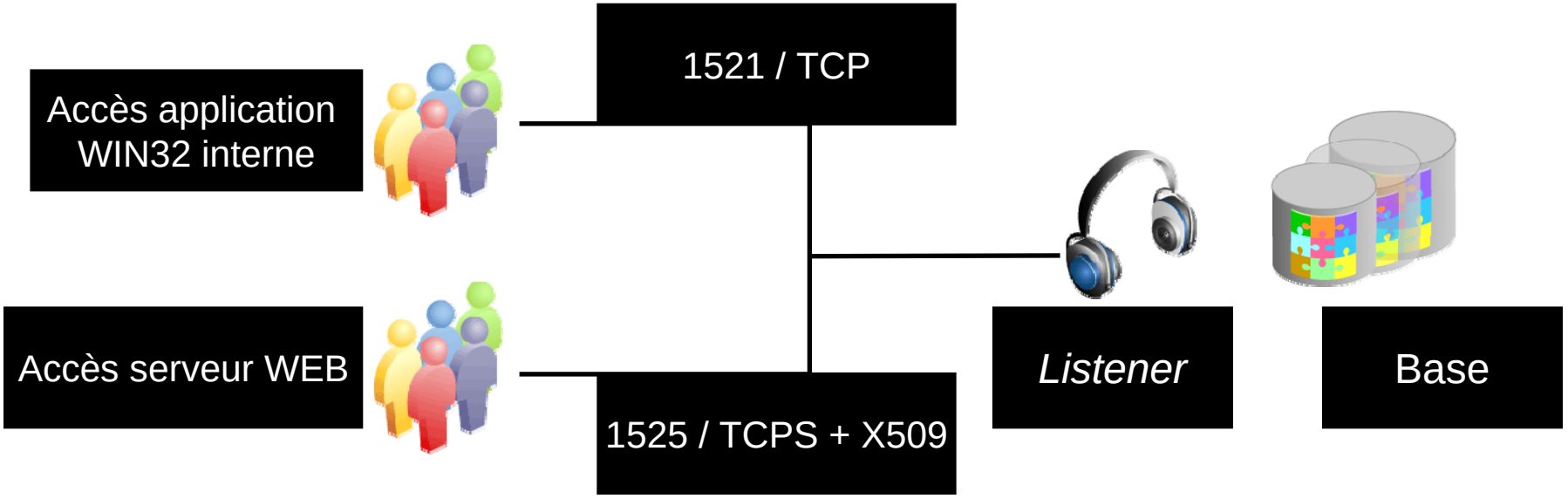


- Protéger les flux *OracleNet*
  - Chiffrement et scellement avec des algorithmes standard *(RC4, 3DES, AES & MD5, SHA-1)*
  - Chiffrement et scellement simple
    - Paramétrage du réseau *OracleNet*
    - Négociation des algorithmes au moment de la connexion
  - Utilisation de TCPS
    - Paramétrage du réseau *OracleNet* et utilisation de certificats. SSL V2 / V3

Chiffrement

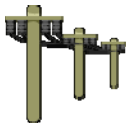
OracleNet

- La sécurisation du réseau d'entrée sur une base peut se faire selon divers protocoles simultanément



Chiffrement

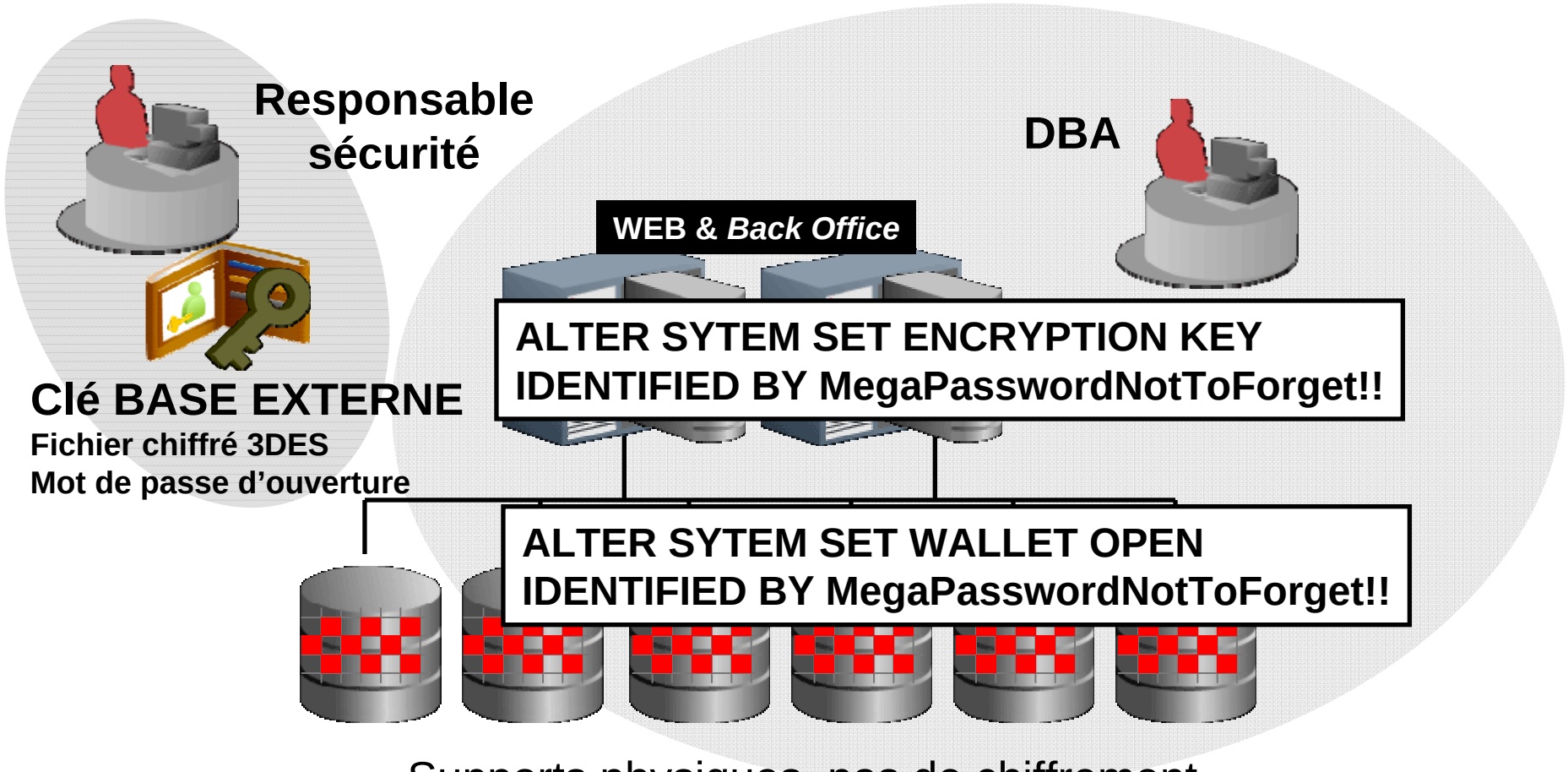
Transparent data Encryption (ASO)



- Protéger les données en stockage
  - La solution devra prendre en charge la gestion des clés de chiffrement
  - Il sera aussi nécessaire d'assurer la séparation des responsabilités entre les administrateurs, les développeurs,
  - …et les personnes en charge de la sécurité des données, donc détentrices des clés d'accès aux données chiffrées

Chiffrement

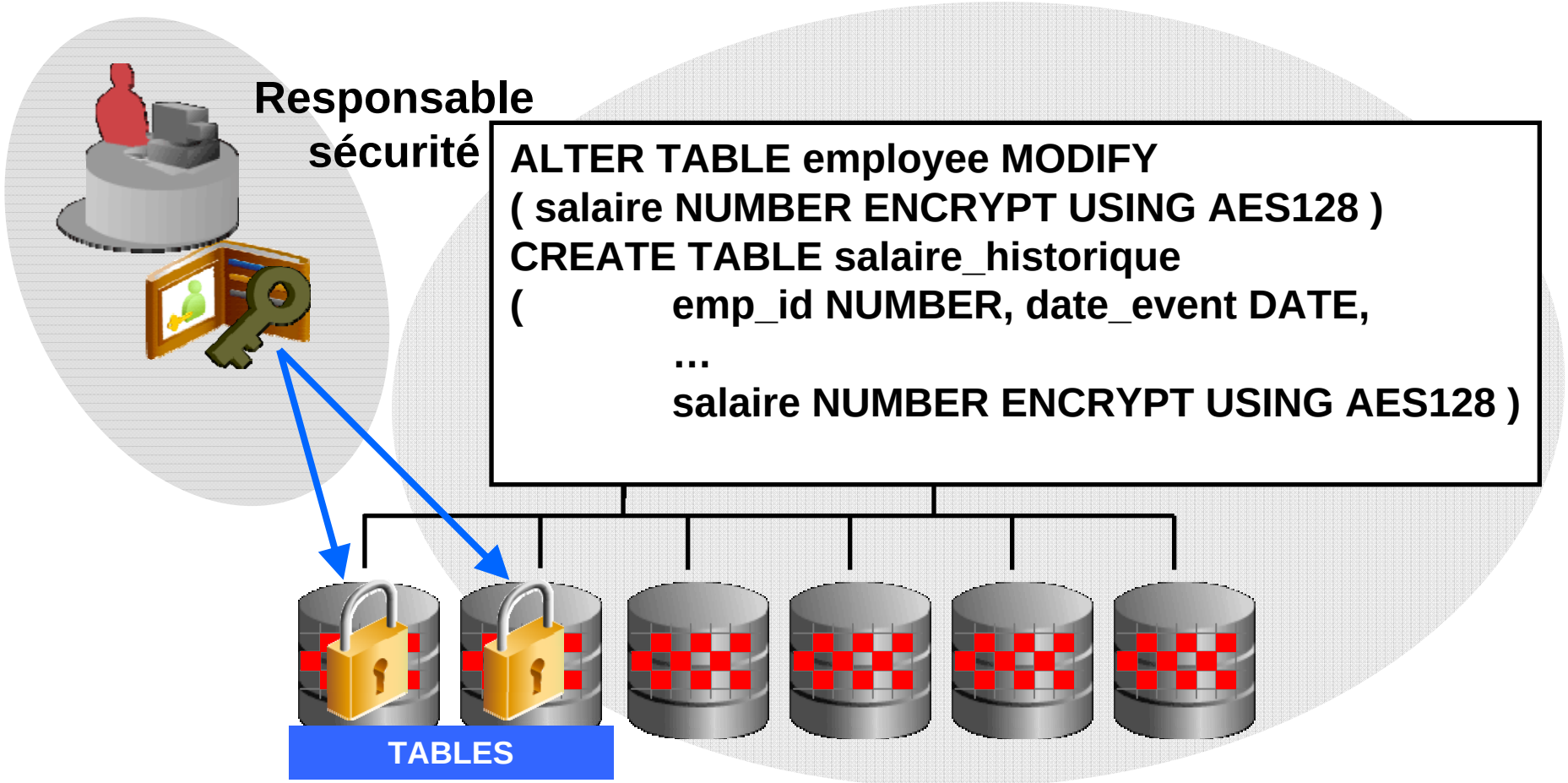
Transparent Data Encryption



Supports physiques, pas de chiffrement

Chiffrement

Transparent Data Encryption

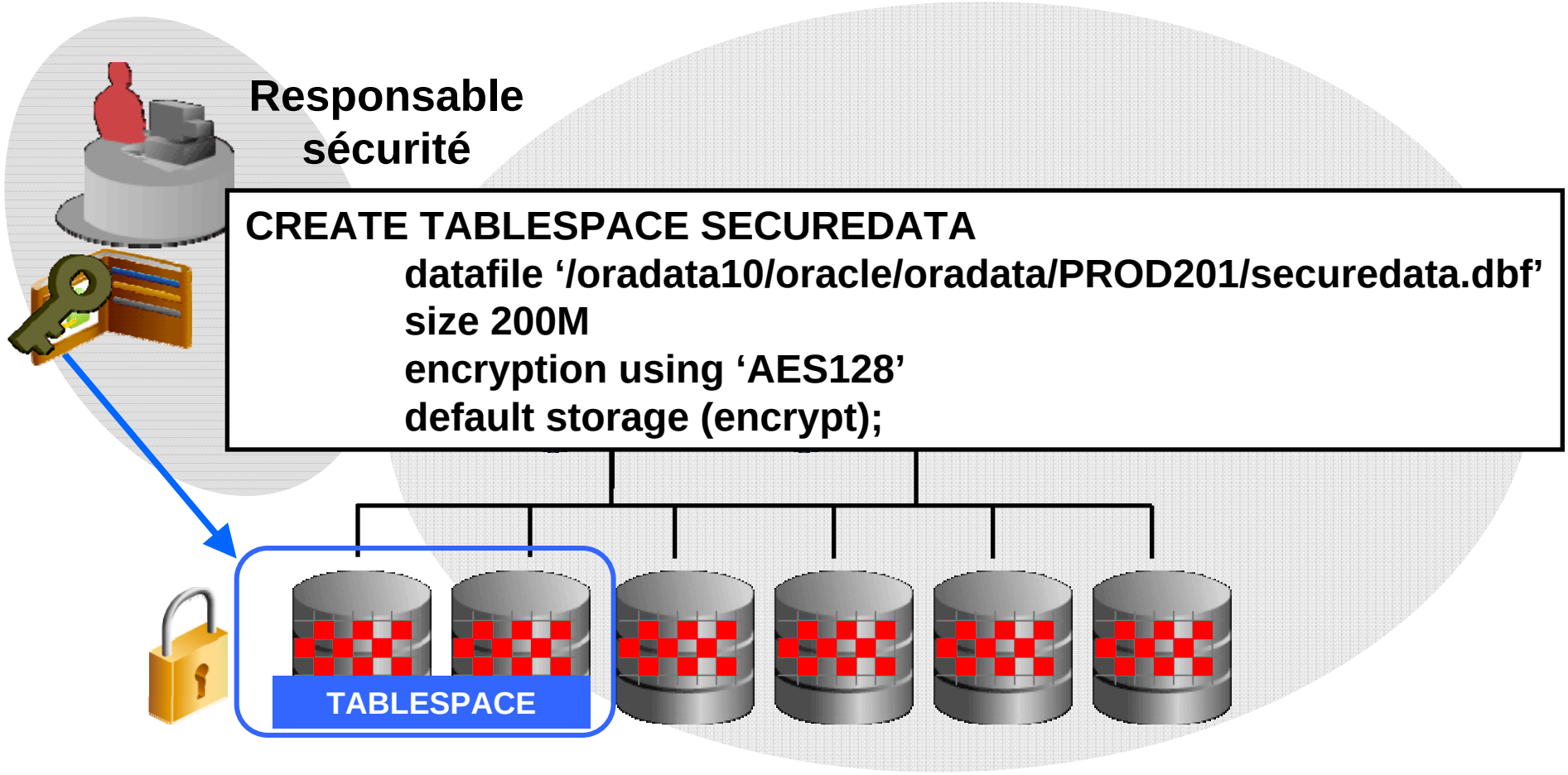


Chiffrement des données de certaines COLONNES sur disque

Chiffrement

Transparent Tablespace Encryption

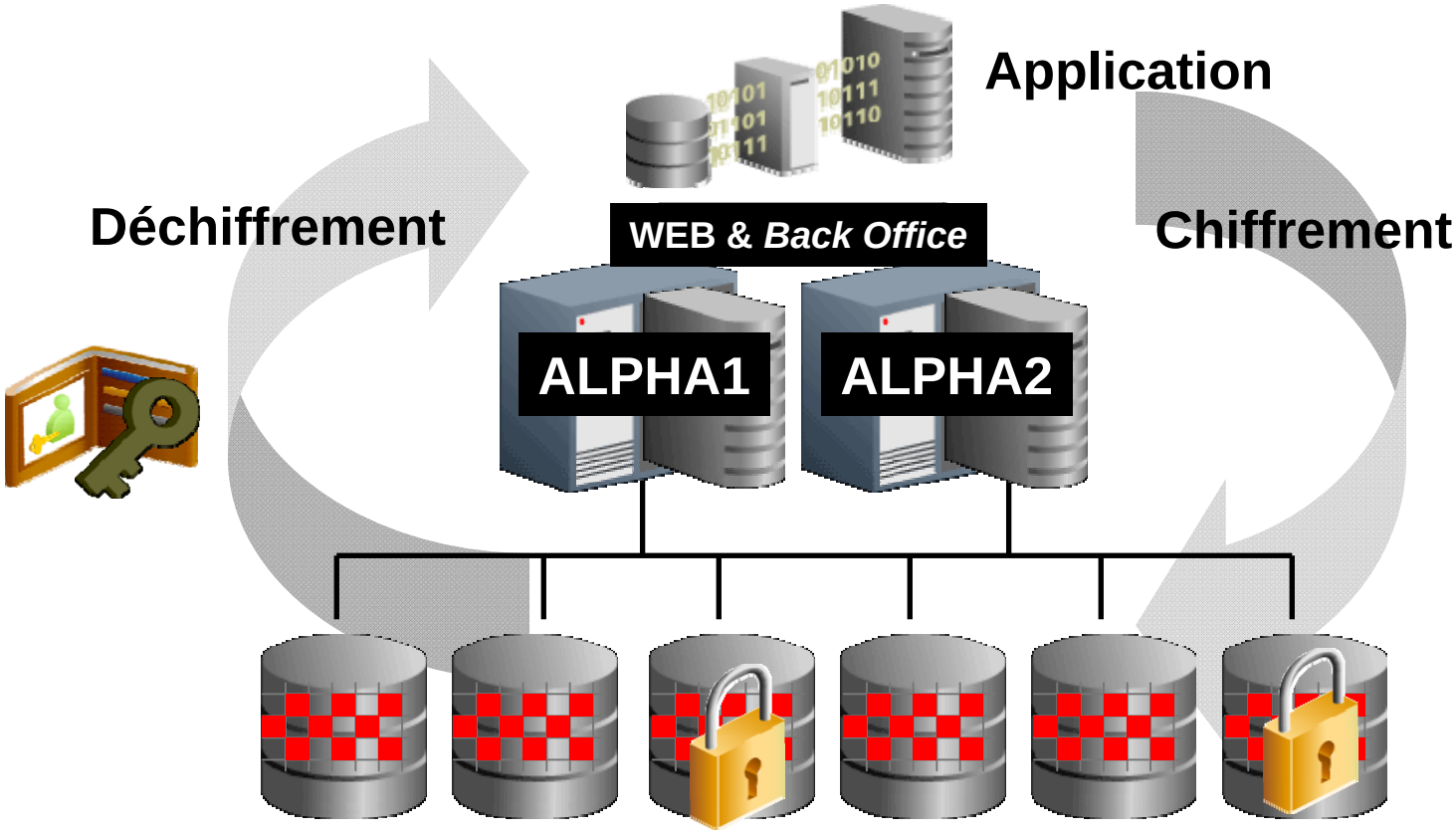
ORACLE DATABASE 11g



Chiffrement des données de certains TABLESPACES sur disque

Chiffrement

Transparent Data Encryption

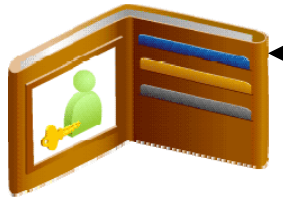


Les données écrites sur les supports physiques sont chiffrées et déchiffrées de façon transparente

Oracle Advanced Security

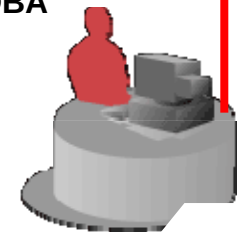
Gestion transparente des clés

Master key stockée dans un wallet PKCS#12 ou un boitier HSM

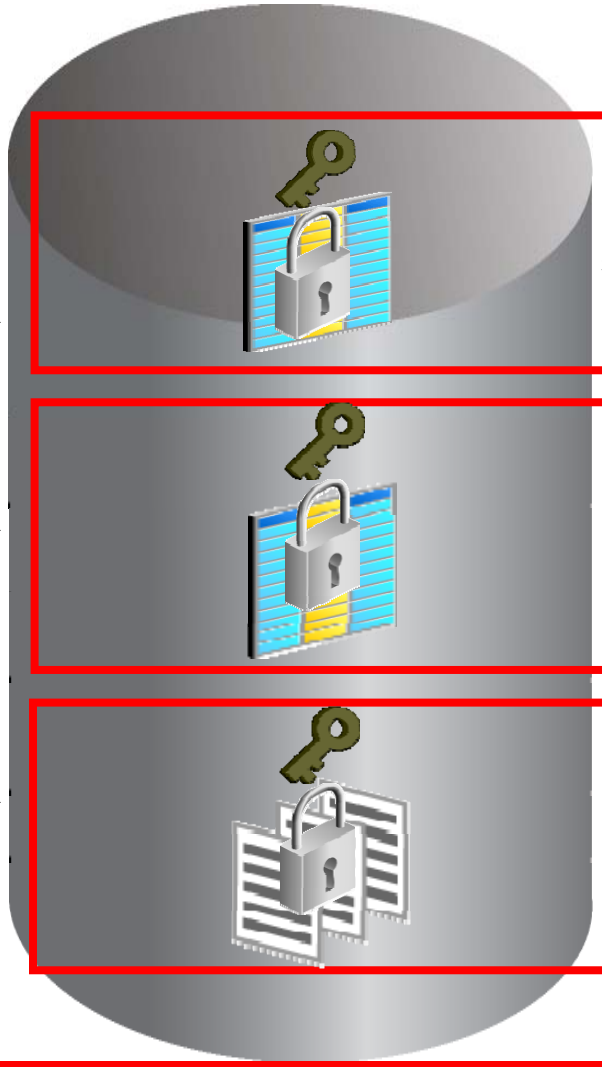


Transparent Data Encryption

Security DBA



Application Users



Les clés de chiffrements des colonnes sont stockées en table et chiffrées avec la master-key

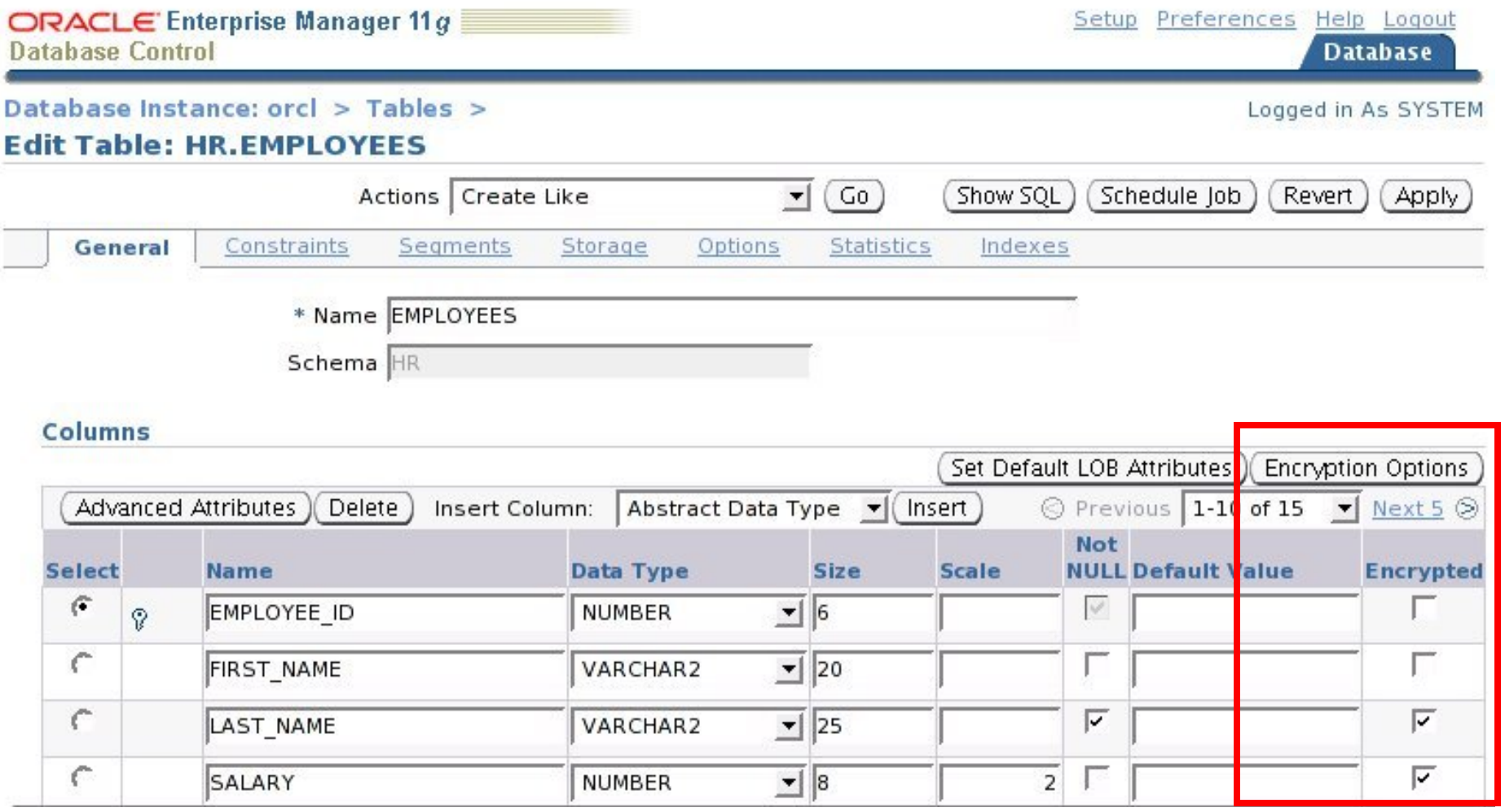
Les données financières FIN sont chiffrées en utilisant la clé de chiffrement de la colonne FIN

Les données de l'application HR sont chiffrées en utilisant la clé de chiffrement du tablespace

Oracle Advanced Security

Cryptage Transparent & Administration (11g)

ORACLE DATABASE 11g



Oracle Advanced Security

Autres évolutions Oracle Database 11g

ORACLE DATABASE 11g

- Cryptage d'un SECUREFILE LOB
- TDE & Integration avec des modules de sécurité Hardware (HSM)
  - Genère, stocke et gère la "master key" dans un périphérique hardware externe
  - L'API au Standard PKCS #11 permet de choisir son matériel hardware de sécurité
- Facilité de mise en œuvre
  - Aucun changement dans les applications existantes
    - Ni triggers, ni vues
    - Impact Minimal sur les performances
    - Gestion de la clé prise en charge

Data Pump et le chiffrement des EXPORTS

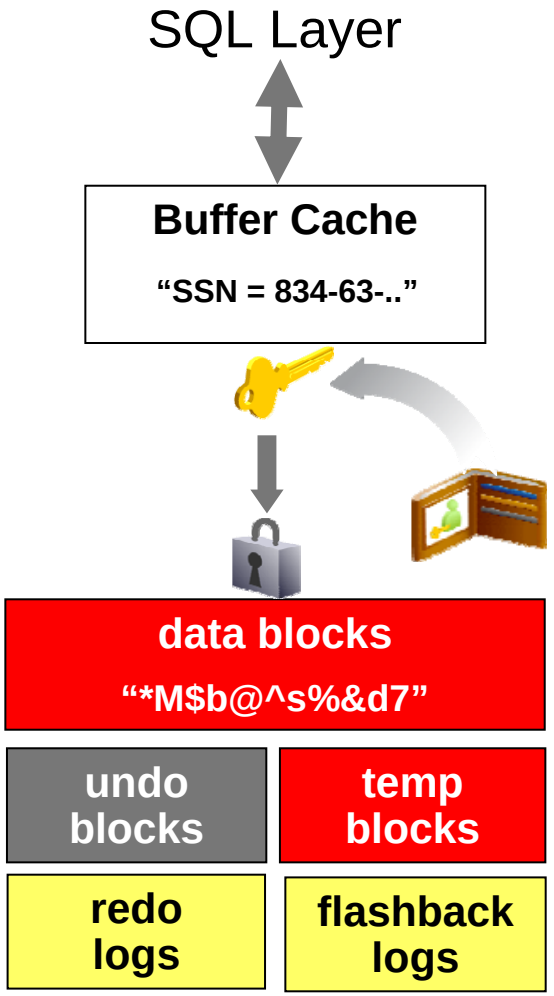
- Exporter les données d'une base les rend vulnérables
- En 10g, expdp sait exporter les données des colonnes chiffrées (paramètre ENCRYPTION_PASSWORD)
- En 11g, on peut chiffrer tout un fichier d'export. Que TDE soit utilisé ou non dans les tables
- La seule contrainte est d'initialiser un WALLET
- Ainsi, on peut ne pas chiffrer dans la base mais protéger les données dès qu'elles en sortent

```
expdp scott/tiger tables=trans …. encryption=data_only
                                  encryption_algorithm=aes128
```

Oracle Advanced Security

Tablespace Encryption

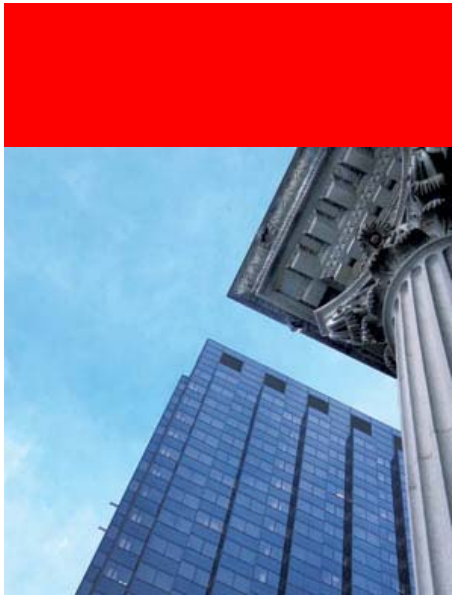
- Chiffrement de toutes les données
  - Chiffre les fichiers bases de données en entier sur l'OS
  - Algorithme standard AES 128
- Efficacité maximale
  - Haute performance
  - Integration avec Oracle Data Compression
- Pas d'impact applicatif



Oracle Advanced Security

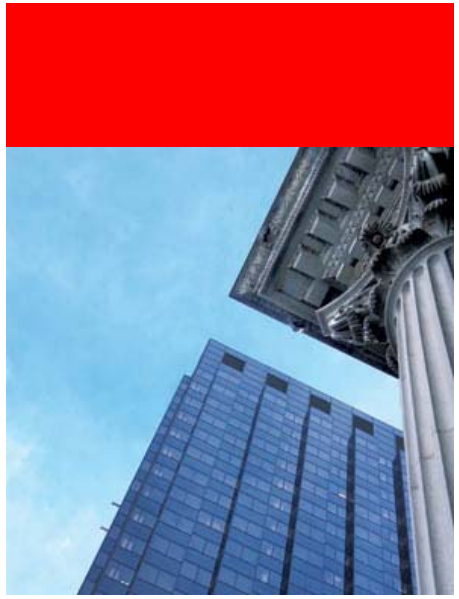
Tablespace Encryption : Performance

- Les blocks de données sont chiffrés / déchiffrés au niveau des E/S Oracle
  - Très Haute Performance (1-2% overhead environ)
  - No index / range scan issues
  - Tous types de données supportés
  - Transparence Complete
- Test dans un contexte Peoplesoft
  - Des tests récent tests utilisant des tablespaces chiffrés dans un contexte applicatif sous PeopleSoft Applications n'ont pas montré des pertes de performance significatives



Démonstration

Chiffrement des données

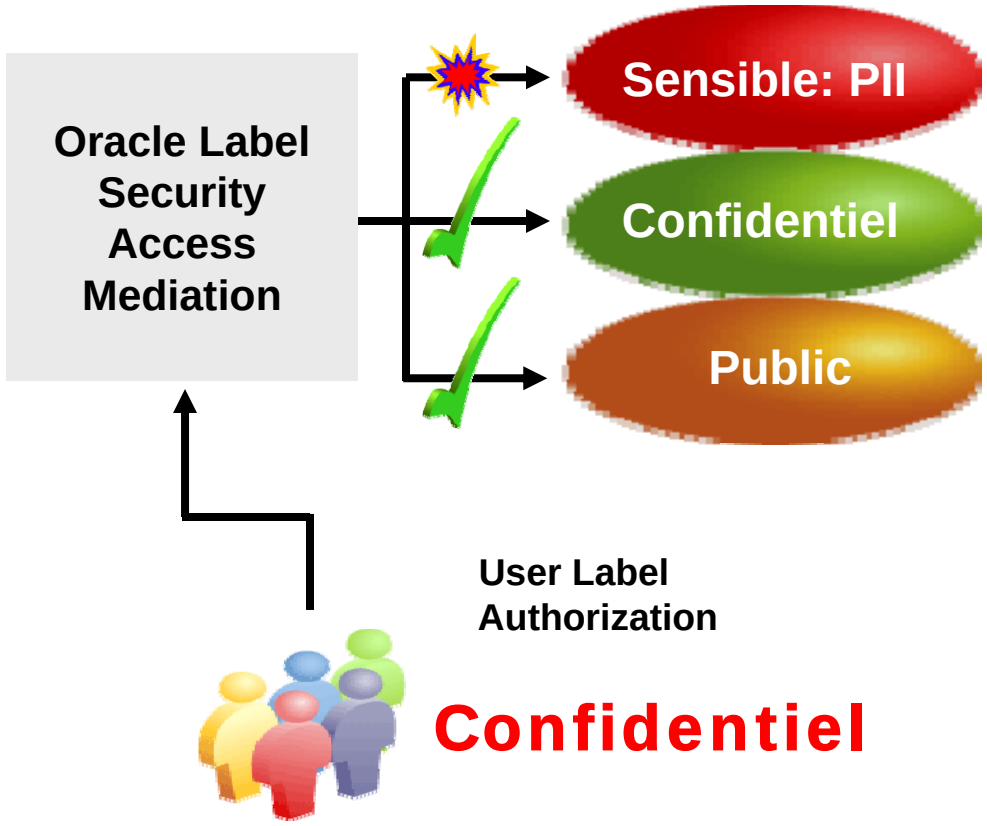


PAUSE

Oracle Label Security

Contrôle d'accès basé sur des labels (étiquettes)

- Etend le système d'autorisation
  - Labelisation des autorisations
- Classification des données
  - Données "sensibles"
- Flexible et Adaptable
  - Utilisateurs Base de Données & Application
  - Options multiples
  - Routines de médiation
  - Disponible depuis Oracle8i



Oracle Label Security

Policy Administration Model

	HR Policy	Law Enforcement Policy	Government Policy
Niveaux	Confidential Sensitive Highly Sensitive	Level 1 Level 2 Level 3	Confidential Secret Top Secret
Catégories	PII Data Investigation	Internal Affairs Drug Enforcement	Desert Storm Border Protection
Groupes	HR REP Senior HR REP	Local Jurisdiction FBI Justice	NATO Homeland Security

Oracle Label Security

Contrôle d’accès basé sur des labels (étiquettes)

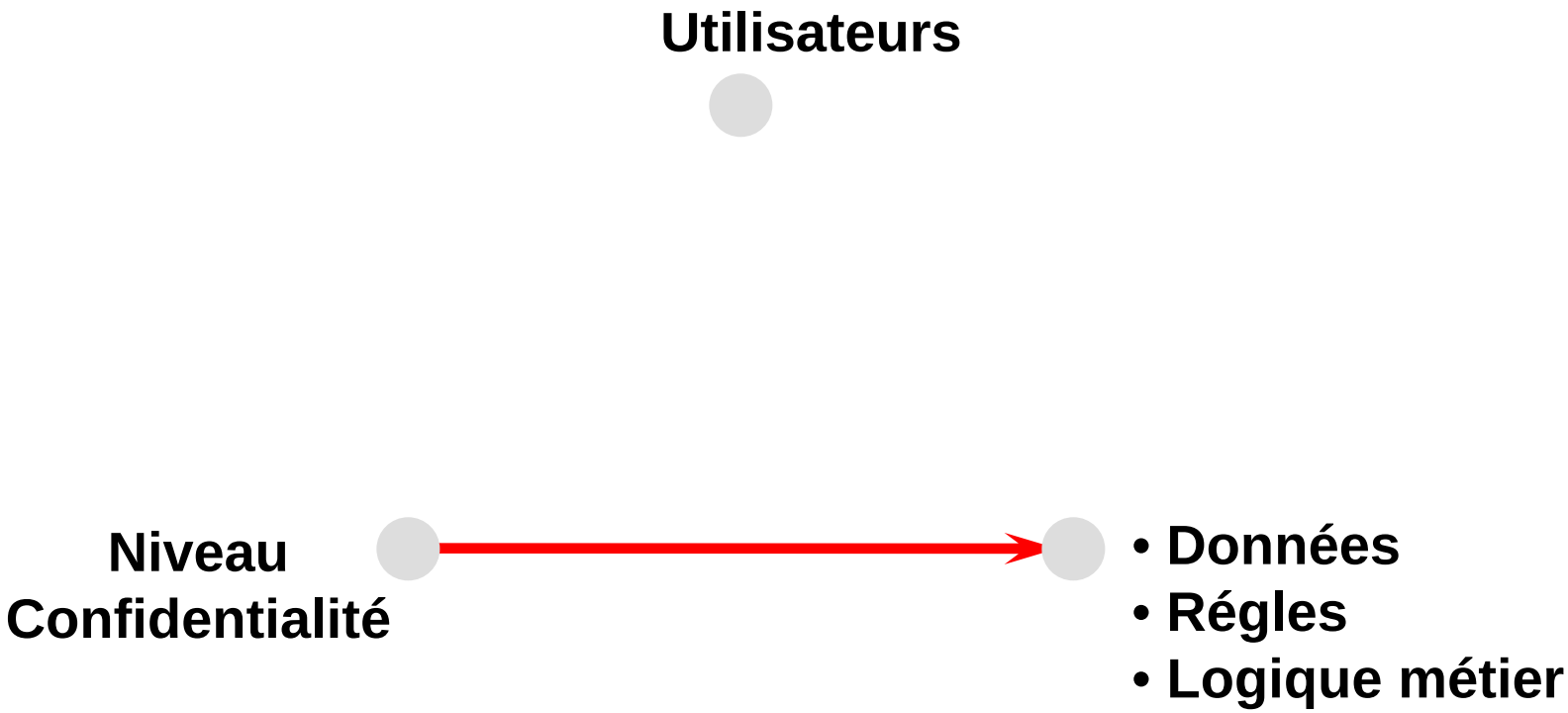
Utilisateurs

Niveau Confidentialité

- **Données**
- **Régles**
- **Logique métier**

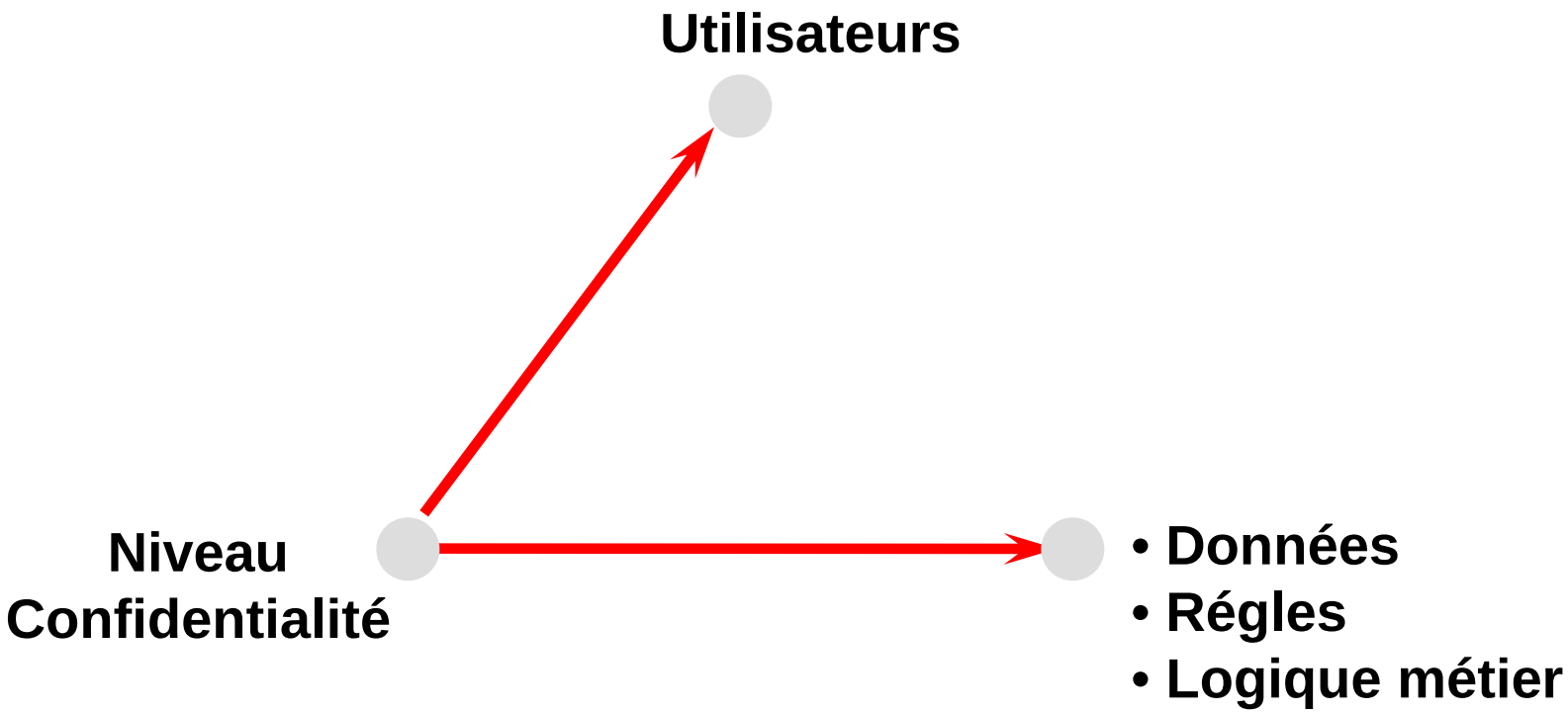
Oracle Label Security

Contrôle d’accès basé sur des labels (étiquettes)



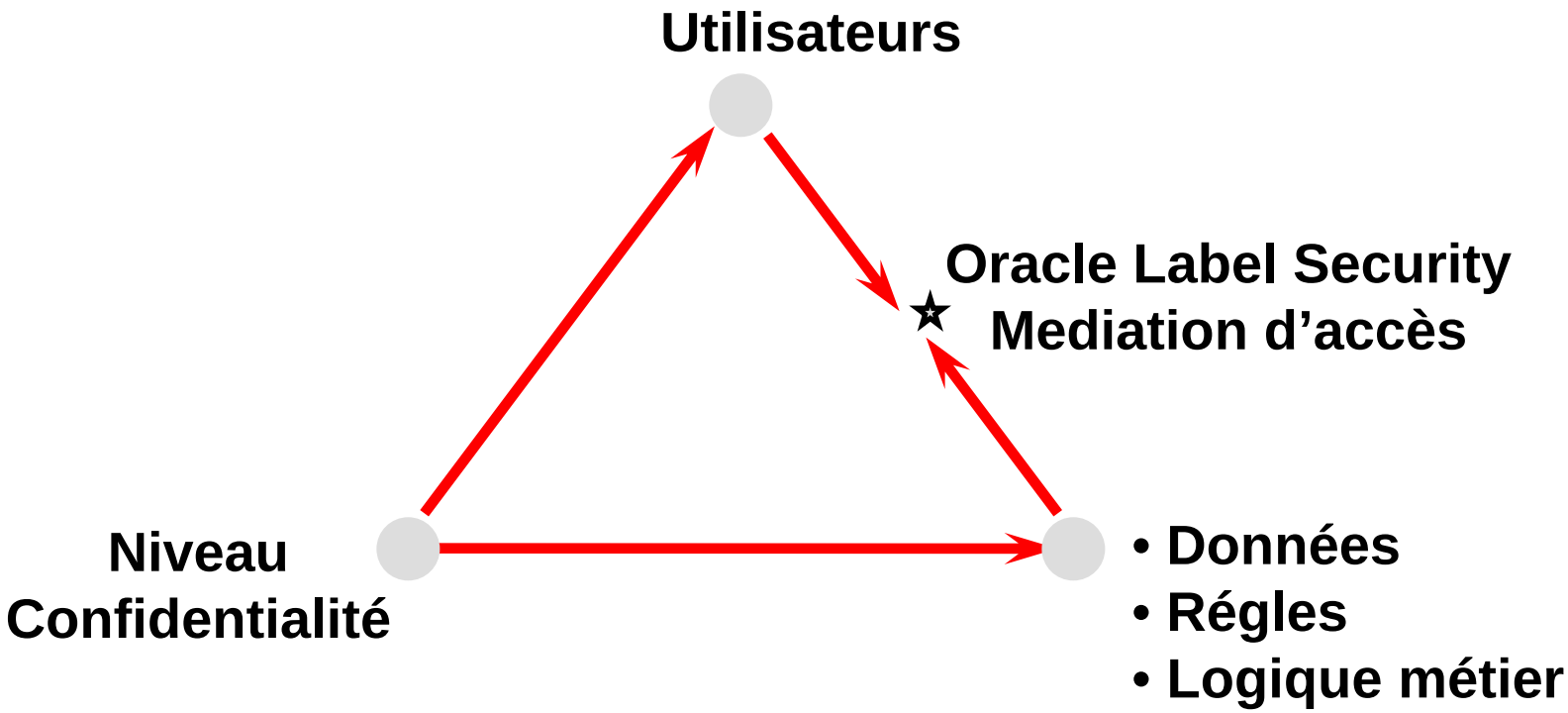
Oracle Label Security

Contrôle d’accès basé sur des labels (étiquettes)



Oracle Label Security

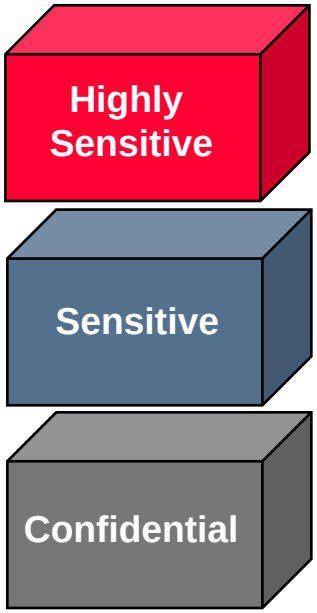
Contrôle d'accès basé sur des labels (étiquettes)



Composants pour la confidentialité

Plus que des niveaux

Niveau Confidentialité

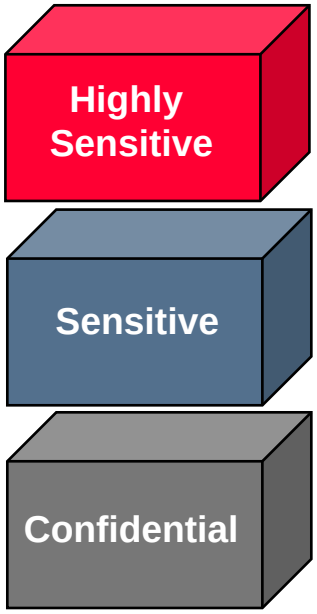


Sensitive

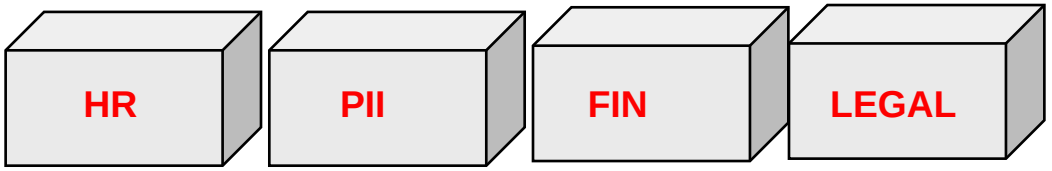
Composants pour la confidentialité

Plus que des niveaux

Niveau Confidentialité



+ Zéro ou plus Catégories

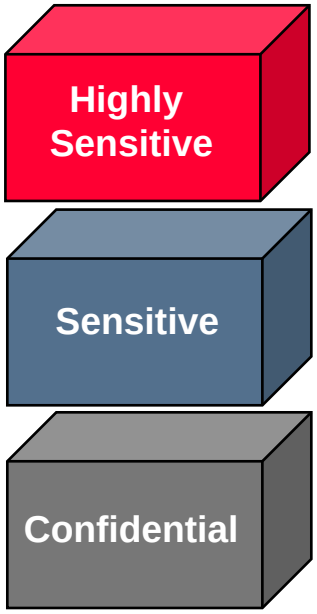


Sensitive : HR

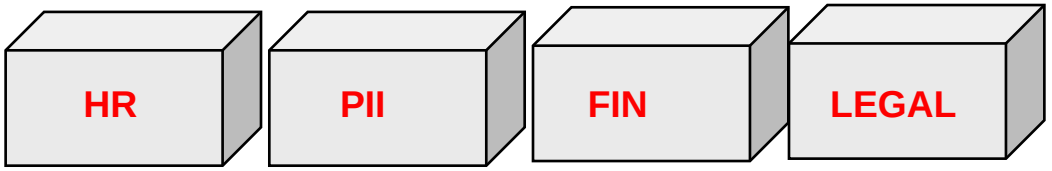
Composants pour la confidentialité

Plus que des niveaux

Niveau Confidentialité



+ Zéro ou plus Catégories



+ Zéro ou plus Groupes

Sensitive : HR : US

Niveaux d'autorisation des Utilisateurs

Obligatoire

User Maximum Level	Highly Sensitive
User Minimum Level	Public
User Default Level	Sensitive
User Default Row Level	Sensitive

User Compartment Authorizations

Optionnel

Compartment	Write	Default	Row
FIN	Yes	Yes	Yes
HR	No	Yes	No

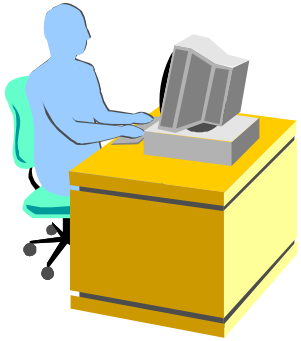
User Group Authorizations

Optionnel

Group	Write	Default	Row
UK	Yes	Yes	Yes
US	No	Yes	No

Oracle Label Security

Sécurité au niveau ligne



Select * from employee_org

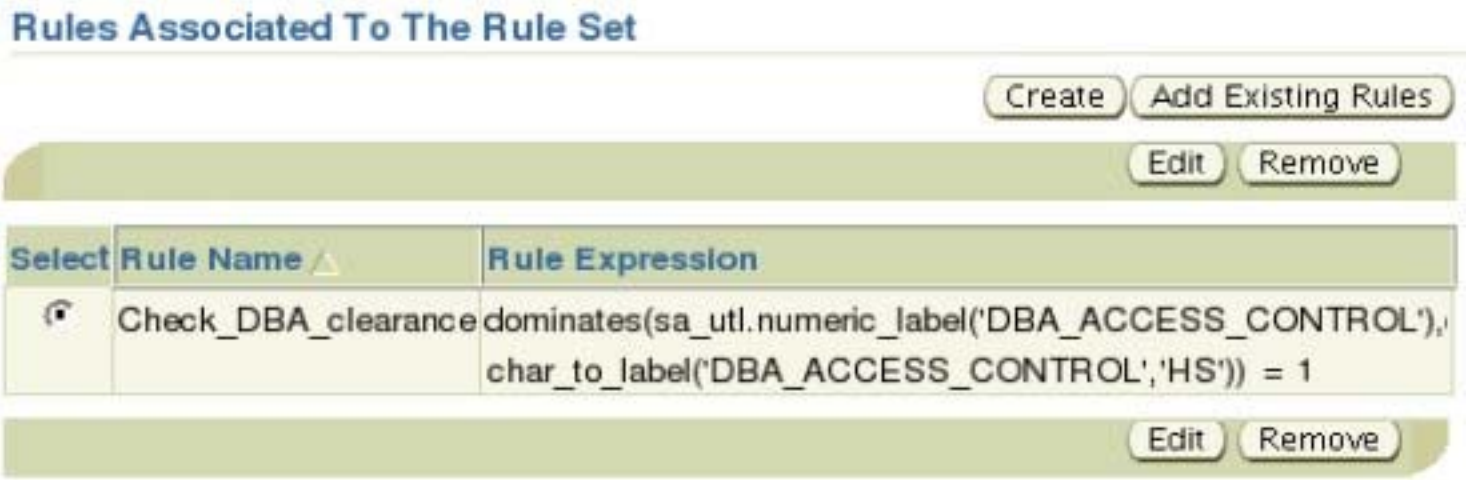
Label Authorization
Sensitive : HR : US

employee_org

LJ1	Confidential
LUS3	Sensitive : HR : US
LUK4	Sensitive : HR : UK

Oracle Label Security

Utilisable avec Database Vault



- La règle examine si le niveau de l'utilisateur courant est supérieur ou égal à 'Highly Sensitive' (HS)
- La règle est associée à un Rule Set
- Le Rule Set est appliqué pour des commandes, par exemple pour la connexion ('connect')
- Seuls les utilisateurs de niveau 'HS' ou plus pourront se connecter

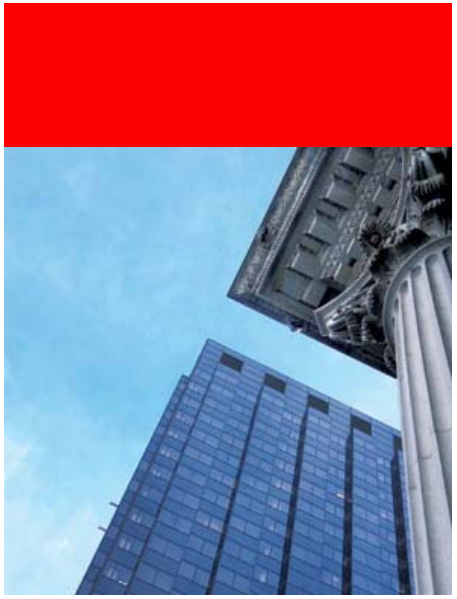
Oracle Label Security

Utilisable avec des règles VPD PL/SQL

- La règle VPD utilise une fonction Label Security

```
if dominates(sa.utl.numeric_label('DBA_ACCESS_CONTROL'),
  char_to_label('DBA_ACCESS_CONTROL','HS') then
        predicate := '1=1';
else
        predicate := '1=2';
End if;
```

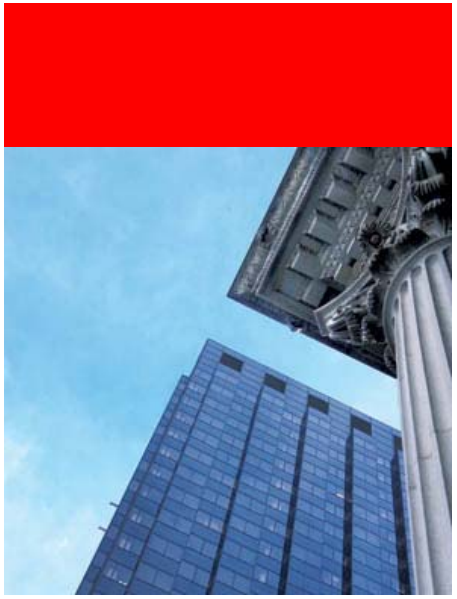
- '1=1' est toujours Vrai: L'accès à la colonne est autorisé quand le niveau de l'utilisateur est suffisant.
- '1=2' est toujours Faux : L'accès à la colonne est interdit quand le niveau de l'utilisateur est insuffisant.



Démonstration

Oracle Label Security

Oracle Data Masking



Démonstration

Oracle Data Masking

Questions